



**Avaya Video Telephony Solution
Release 4.0
Networking Guide**

16-601423
Issue 3
January 2008

© 2008 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

For full legal page information, please see the complete document, Avaya Legal Page for Software Documentation, Document number 03-600758.

To locate this document on the website, simply go to <http://www.avaya.com/support> and search for the document number in the search box.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site:

<http://www.avaya.com/support>

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site:

<http://www.avaya.com/support>

Contents

Chapter 1: Introduction	7
Overview of Avaya Video Telephony Solution	7
What's New in this Release	8
Requirements	8
Managing Video on Your Network	9
Classifying Video Users	9
Set Up Your Bandwidth Pools	10
Sample Scenarios	10
Chapter 2: Design and Deployment Checklist.	17
Overview	17
Network and PBX-Network Requirements	18
Feature Interactions and Limitations	20
Avaya Communication Manager Global Administration	21
Avaya Communication Manager Administration for Ad-hoc Video Conferencing	27
Avaya Communication Manager Administration for Polycom Multipoint Stations (VSX and HDX)	28
Avaya Communication Manager Administration for Polycom MGC Systems . . .	29
Avaya Communication Manager Administration for Polycom RMX Systems . . .	32
Polycom MGC Configuration	33
Polycom RMX Configuration	35
Polycom VSX System Configuration	37
Avaya IP Softphone (IPSP)	38
Avaya IP Softphone Performance Issues	41
Priority Bandwidth Management	42
SIP Administration (Global).	43
SIP Trunk Administration	44
SIP Station Administration (OPTIM)	45
SIP Limitations.	46

Chapter 3: Setting Up Video Endpoints	47
Required Administration	48
Configure IP Codec Sets	48
Configure IP Network Regions	50
Configure a Station Endpoint for Avaya IP Softphone Release 6.0 and Video Integrator	53
Checklist	53
Configuration Procedures.	53
Configure Polycom VSX/HDX Series Video Conferencing Systems and V500/V700 Video Calling Systems	57
Checklist	57
Configuration Procedures.	57
Configure a Polycom RMX Series Video Conferencing Bridge Platform	65
Checklist	65
Configuration Procedures.	65
Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform	71
Checklist	71
Configuration Procedures.	71
Display Capacity for Ad-hoc Video Conferencing.	77
View Video Conferencing Bridges	77
Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server.	78
Checklist	78
Configuration Procedures.	78
Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server	82
Trunk Groups	82
Signaling Groups	83
Group Member Assignments	84
Outgoing Rules	85
Examples	86
Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform	89
Checklist	89
Configuration Procedures.	89
Display Capacity for Ad-hoc Video Conferencing.	95
View Video Conferencing Bridges	95

Configure an Avaya Meeting Exchange 5.0.1 S6800 Bridge	96
Checklist	96
Things to Keep in Mind	96
Configuration Procedures.	97
Configure a Polycom MGC Video Conferencing Bridge Platform as an H.320 Gateway	126
Trunk Groups	126
Route Pattern	127
AAR Tables.	127
MGC Administration	127
Configure a Polycom PathNavigator/SE200 Gatekeeper	128
Checklist	128
Configuration Procedures.	128
Configure Video Trunks between Two Avaya Communication Manager Systems	131
Checklist	131
Configuration Procedures.	131
Monitor the Status of Video Bandwidth Usage	134
Index	135

Chapter 1: Introduction

Overview of Avaya Video Telephony Solution

The Avaya Video Telephony Solution enables Avaya Communication Manager to merge a set of enterprise features with Polycom's videoconferencing adjuncts. It unifies voice over IP with video, web applications, Avaya's video-enabled IP Softphone, third-party gatekeepers, and other H.323 endpoints. With the Avaya Video Telephony Solution, you can provide video for desktop and group communications.

The Avaya Video Telephony Solution supports video calls on the following products:

- Avaya IP Softphone Release 6.0 and Video Integrator
- Polycom HDX series video conferencing system
- Polycom VSX series video conferencing system
- Polycom V500/V700 video calling system
- Polycom RMX series video conferencing bridge platform
- Polycom MGC video conferencing bridge platform
- Avaya Meeting Exchange 5.0.1 S6800 bridge
- third-party gatekeepers, including Polycom PathNavigator/SE200 gatekeepers
- H.320 gateways

Note:

You must perform a network readiness or network assessment to ensure your network is capable of supporting the high bandwidth demands of video over IP. You should also consider implementing QoS across your network.

What's New in this Release

Avaya Video Telephony Solutions Release 4.0 introduces the following new features and enhancements:

- Ability to support Ad-hoc video conferencing with Polycom MGC systems, Polycom RMX systems, and Avaya Meeting Exchange 5.0.1 systems.
- Ability to support the Polycom RMX series video conferencing bridge platform.
- Ability to support the Polycom HDX series video conferencing system.
- Ability to support SIP video telephony with Avaya DevConnect-approved SIP video endpoints and Avaya Meeting Exchange 5.0.1 bridges.

Requirements

Video Telephony Solution Release 4.0 requires:

- an S8xx server that is running Avaya Communication Manager software release 5.0.
- Avaya-enabled Polycom MGC Manager software installed and running.
- Avaya licensing keys (for RMX and HDX systems)

Managing Video on Your Network

Before configuring video endpoints, you should determine how you want to manage video on your network. To control how your bandwidth is used, you must:

1. Determine whether you want to provide some endpoints with video whenever possible.
2. Set up your bandwidth pools.

Classifying Video Users

You can identify two types of video stations: priority video stations and normal video stations. Priority stations have an increased likelihood of receiving bandwidth and may also be allocated a larger maximum bandwidth per call. By having a larger maximum bandwidth per call, priority video stations may receive better quality and more reliable video during calls. Priority video stations will have an increased likelihood of having video on outgoing calls they make. However, they might not receive video on incoming calls they receive from “non-priority” stations due to the following conditions:

- No bandwidth is available.
- No “normal” bandwidth is available even though priority bandwidth is available. Since the call is made by a normal (non-priority) video station, this station would not have access to the priority bandwidth.

These non-priority stations are referred to as “normal” stations. Normal video stations may or may not get video, depending on the available bandwidth.

Set Up Your Bandwidth Pools

Bandwidth pools enable you to control video usage for normal video users and priority video users. You can divide the bandwidth into three pools:

- **Audio pool**
The audio pool contains bandwidth for all audio calls, including the audio-component of multimedia calls.
- **Normal video pool**
The normal video pool contains bandwidth for the video portion of a call made by a normal (non-priority) video user. You can set this pool to be shared. When this pool is shared, audio-only calls are allowed to borrow bandwidth from this pool.
- **Priority video pool**
The priority video pool contains bandwidth that is dedicated to priority video users only. Audio calls and normal video users are not allowed to borrow bandwidth from this pool. However, if all of the priority video pool bandwidth is currently in use, priority video users can borrow bandwidth from the normal video pool, if available.

Sample Scenarios

This section provides some examples of how you could specify the bandwidth settings for your network.

Example 1

In this example, you do not want to allocate any bandwidth for video. You want to configure the network to use IP audio. [Figure 1](#) shows how you would configure the bandwidth pools for this example.

Table 1: Bandwidth Settings for Example 1

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	3 Mb	0 Mb	0 Mb	No

Example 2

In this example, your network has unlimited bandwidth. Since all of your users can get as much bandwidth as they need, there is no need to specify priority users. There is only one pool of bandwidth to be shared by audio and multimedia calls. Audio will come from the normal video pool. [Figure 2](#) shows how you would configure the bandwidth for this example.

Table 2: Bandwidth Settings for Example 2

Total Bandwidth	Audio Bandwidth Pool	Priority Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0 Mb	0 Mb	3 Mb	Yes

Example 3

In this example, you have bandwidth for video only, and you want to reserve some bandwidth for the CEO. All voice calls will be routed another way. You want to reserve half of your bandwidth (1.5 Mb) for priority users. If priority users need more than 50% of the bandwidth, they will be able to use the available bandwidth from the normal video pool. Audio will come from the normal video pool. [Figure 3](#) shows how you would configure the bandwidth for this example.

Table 3: Bandwidth Settings for Example 3

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0 Mb	1.5 Mb	1.5 Mb	No

Example 4

In this example, you do not want to use too much bandwidth on audio. You want to reserve most of the bandwidth for video, but you want to allow a few audio calls to keep costs down. You have a small number priority users. [Figure 4](#) shows how you would configure the bandwidth for this example.

Table 4: Bandwidth Settings for Example 4

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	No

The settings in table will allow a few audio calls and one or two priority calls depending on the bit rate. After the audio pool runs out of bandwidth, the calls will be forced to take another route since the normal video bandwidth pool is not shared. If a priority call occurs when all of the priority video bandwidth is used, it will use any available bandwidth in the normal video bandwidth pool before using bandwidth from the audio bandwidth pool.

Example 5

In this example, you do not want to use any IP bandwidth for audio. You want to use IGAR for audio. All IP bandwidth will be used for video. [Figure 5](#) shows how you would configure the bandwidth for this example.

Table 5: Bandwidth Settings for Example 5

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0 Mb	0 Mb	3 Mb	No

Since you have allocated no audio bandwidth, audio calls will fall over to the public-switched telephone network. However, multimedia calls will take audio bandwidth and video bandwidth from the normal video bandwidth pool.

Example 6

In this example, you want video only for the Polycom VSX systems in the boardroom and in the CEO's office. Also, this bandwidth must be available always. There are no normal video users. The extensions for the Polycom VSX systems are administered for priority video. [Figure 6](#) shows how you would configure the bandwidth for this example.

Table 6: Bandwidth Settings for Example 6

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	2.1 Mb	0.9 Mb	0 Mb	No

Example 7

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You do not want to share the normal video bandwidth pool because you have very strict limitations on the bandwidth.
- You do not want to exceed any of the provisioned pools.

[Figure 7](#) shows how you would configure the bandwidth for this example.

Table 7: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0 Mb	2.1 Mb	No

Example 8

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You do not want to share the normal video bandwidth pool because you have very strict limitations on the bandwidth. By not sharing the normal video bandwidth pool, you guarantee:
 - a minimum level of video bandwidth
 - audio-only calls cannot impact the normal video bandwidth pool
- You do not want to exceed any of the provisioned pools.
- You want to specify a proportion of priority video users.

[Figure 8](#) shows how you would configure the bandwidth for this example.

Table 8: Bandwidth Settings for Example 8

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	No

In this example, 600 Kbit is reserved for priority video. A priority video user will be able to use the normal video pool if the priority pool is all used and bandwidth exists in the normal video pool.

Example 9

In this example, the following conditions exist:

- You want to share the normal video bandwidth pool.
- You have no priority video users.

[Figure 9](#) shows how you would configure the bandwidth for this example.

Table 9: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0 Mb	2.1 Mb	Yes

Since there are no priority video users, the normal video bandwidth pool is the entire video bandwidth pool. With no priority users and the bandwidth being shared, all of the bandwidth could be used as audio.

Example 10

In this example, the following conditions exist:

- You want to guarantee a certain audio bandwidth and video bandwidth.
- You want to share the normal video bandwidth pool.
- You have priority video users.

[Figure 10](#) shows how you would configure the bandwidth for this example.

Table 10: Bandwidth Settings for Example 7

Total Bandwidth	Audio Bandwidth Pool	Priority Video Bandwidth Pool	Normal Video Bandwidth Pool	Share Normal Video Bandwidth Pool
3 Mb	0.9 Mb	0.6 Mb	1.5 Mb	Yes

In this example, 600 Kbit of bandwidth is reserved for priority video users. Audio cannot use this bandwidth. The maximum available bandwidth for audio is 2.4 Mb. (In this case, there would be no normal video bandwidth available.) The maximum available bandwidth for priority video users is 2.1 Mb.

Chapter 2: Design and Deployment Checklist

Overview

The chapter provides a checklist that will help you design and deploy the Avaya Video Telephony Solution R4.0.

Note:

For the latest firmware video compatibility matrix, go to **www.avaya.com/support**. and access Video Telephony Solution.

Network and PBX-Network Requirements

Question 1: Has a multimedia QoS policy been designed and deployed?

- ☐ **Yes.**
- ☐ **No.** Avoid best effort treatment of video. Avaya IP Softphone (IPSP), Polycom MGC, Polycom RMX, and Polycom VSX all support QoS for video. See the checklist in section 11.0 of the white paper from Polycom Global Services titled “Supporting Real-time Traffic: Preparing Your IP Network for Video Conferencing.”

Question 2: Has a default enterprise Maximum Call Rate been selected?

Note:

Use **change ip-codec-set** and enable “Allow Direct IP Multimedia” on page 2 of the form. In Avaya Communication Manager Release 4.0, there are two options: Normal users and Priority users.

- ☐ **Yes.**
- ☐ **No.** Recommend initial deployment with Maximum Call Rate of 384 Kbps.

Note:

Keep in mind the following:

- Allow for 20% for IP protocol overheads.
- High definition room systems support call rates of 4 Mbps.

Question 3: Is inter-PBX network connectivity less than 150 ms end-to-end one-way delay and less than 1% packet loss at all times?

- ☐ **Yes.**
- ☐ **No.** Expect slower call establishment. Compared to audio-only calls, multimedia calls have a greater number of round-trip signaling messages by a factor of 5.

Question 4: Does the VPN connection for Avaya IP Softphone have less than 150 ms one-way delay to Avaya Communication Manager, is packet loss less than 1%, and is jitter less than 20 ms?

☐ **Yes.**

☐ **No.** Avaya IP Softphone does not support automatic bit rate downgrades on packet loss feedback, nor does it perform ping tests for video assessment. The user must reduce call rate and reattempt the call to achieve the best video experience for the network conditions. In worst-case conditions, users may experience video disablement by Avaya Communication Manager for the call duration due to excessive video update requests.

Question 5: Are there video call scenarios that would cross more than three Avaya Communication Manager systems?

Note that a limitation of the solution is that shuffling to direct-ip is blocked for Avaya Communication Manager systems that are pushing tandem trunk-to-trunk multimedia calls. Hairpinning is allowed.

☐ **Yes.** Administer additional trunks to minimize the use of tandem Avaya Communication Manager systems, thereby reducing video-update latency. Avoid the use of slow CPU servers (for example, S8700) in tandem scenarios, since video signaling across many Avaya Communication Manager systems is exponentially more expensive than audio-only calls.

☐ **No.**

Feature Interactions and Limitations

Question 1: Is Call Recording, Whisper Page, or Service Observing going to occur on video calls?

☐ **Yes.** Expect audio-only calls. It is working as designed. From Avaya Communication Manager Release 5.0, the ad-hoc video conferencing feature may resolve some of these limitations.

☐ **No.**

Question 2: Is “transfer to MGC/RMX” being used for ad-hoc conferencing?

☐ **Yes.** Avoid scenarios where a user attempts to transfer to a meeting room where tandem Avaya Communication Manager systems link the user to the Polycom MGC/RMX. Multiple Avaya Communication Manager shuffling (if allowed) may legitimately block the transfer. A reattempted transfer should succeed.

☐ **No.**

Question 3: Should a customer with a network of PBXs trunked together who will want to deploy ad-hoc video conferencing with Polycom RMXs in the future deploy those RMXs in a distributed manner?

☐ **Yes.** Ad-hoc conferencing will require at least one Polycom RMX per active Avaya Communication Manager system to support future ad-hoc video conferencing via the Conference button.

☐ **No.**

Question 4: Have additional media resources been allocated for Avaya Communication Manager systems that are used for tandem multimedia calls?

In a typical hub and spoke arrangement of Avaya Communication Manager systems, the core PABX that is doing the tandem calls between remote PABX systems should have additional media resources deployed as shuffling to direct-ip is blocked for multimedia calls.

☐ **Yes.**

☐ **No.** Expect higher utilization of media resources on tandem Avaya Communication Manager systems.

Avaya Communication Manager Global Administration

Question 1: Are the video capacities on system-parameters customer-options, page 2 configured correctly?

Maximum Video Capable H.323 Stations should be 1 x the number of single point Polycom VSX systems .

Maximum Video Capable IP Softphones should be equal to the number of video softphones.

Maximum Administered Ad-hoc Video Conferencing Ports should be based on the number of RMX systems and the maximum port count capability for the RMX systems.

☐ Yes.

☐ No.

Question 2: Are the fields on system-parameters customer-options, page 4 configured correctly?

“Enhanced Conferencing?” = **y**

“IP Trunks?” = **y**

“IP Stations?” = **y**

“ISDN-BRI Trunks?” = **y**

“ISDN-PRI?” = **y**

“Multimedia Call Handling (Basic)?” = **n**

“Multimedia Call Handling (Enhanced)?” = **n**

☐ Yes.

☐ No.

Question 3: Are the fields in ip-network-region, page 1 configured properly for all regions used by video endpoints?

"Intra-region IP-IP Direct Audio" = **y**

"Inter-region IP-IP Direct Audio" = **y**

Note:

For network regions containing third-party gatekeepers, these values must be set to **No** for direct audio because shuffling may not be supported by all third-party endpoints.

☐ **Yes.**

☐ **No.** Note the actual settings in this page and find out the customer's reasons/requirements for these options to be disabled. Video endpoints do not need to be shuffled to resume video. Third-party endpoints will support basic call setup only.

Question 4: Are the fields in ip-network-region, page 2 configured properly for all regions used by video endpoints?

H.323 SECURITY PROFILES must contain **any-auth** for Polycom VSXs to authenticate. **challenge** is used by Avaya IP Softphone. **pin-cke** is used by Polycom VSX. **any-auth** encompasses both **challenge** and **pin-cke**.

☐ **Yes.**

☐ **No.** Expect registration failures.

Question 5: Is the ip-codec-set form configured properly?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, trunks, and stations as well as inter-region codec sets. Has the enterprise selected a single version of G.711 across all Avaya Communication Manager systems globally?

☐ **Yes.**

☐ **No.** Simplify the codec-set administration by selecting one variant of G.711 across the entire network of Avaya Communication Manager systems. **A single variant can be used globally.** Otherwise expect codec mismatch errors and call drops between Avaya Communication Manager systems. Multimedia signaling uses H.245, which is more sensitive to codec administration than audio-only repeat-fast start signaling.

Question 6: Is the intra-region audio administration correct in the ip-codec-set form?

Review all IP codec-sets used across the enterprise including the IP codec-sets used by media processors, IP trunks, and IP stations.

Wide-band codecs (for example, SIREN series, G.722.1 series, and G.722-64k) should appear first and are supported for shuffled Polycom VSX calls only across a single Avaya Communication Manager system.

G.711 should appear next.

Then follow with G.729/G.729A codec, etc.

☐ **Yes.**

☐ **No.**

Question 7: Is the inter-region audio administration correct in the ip-codec-set form?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, IP trunks, and IP stations.

Are there bandwidth issues? If no, then re-use the one codec set also in use for intra-region.

If there are bandwidth issues, specify a low bandwidth codec first followed by one G.711 codec. If there are severe bandwidth issues, customers can choose to leave out G.711 and also ensure video is disabled.

☐ **Yes.**

☐ **No.**

Question 8: Is the audio administration for Polycom VSXs correct in the ip-codec-set form?

Review all codec-sets used across the enterprise including the codec-sets used by media processors, trunks, and stations.

If codec-sets used for stations include G.729, then a new network-region and codec must be defined for use by Polycom VSXs. VSX stations do not support G.729 but do support G.729A.

Note that media encryption is not supported by VSX stations.

☐ **Yes.**

☐ **No.** Expect call setup failure. This is a work around for a VSX signaling issue.

Question 9: Is the video administration correct in the ip-codec-set form?

Review page 2 of all the codec-sets to be used by video stations and video trunks.

Is “Allow Direct-IP Multimedia?” set to **yes**?

Is “Maximum Call Rate for Direct-IP Multimedia” set appropriately considering whether the codec-set is used for inter-region where there are bandwidth issues.?

- ☐ **Yes.**
- ☐ **No.** Expect audio only calls.

Question 10: Is ip-network-region inter-region video bandwidth management used across WAN links?

Ensure appropriate video total bandwidth limits on ip-network-region page 3 are set correctly.

- ☐ **Yes.**
- ☐ **No.** Expect low-quality video. Avaya recommends replacement of CAC via trunk-member counting with cumulative bandwidth management. Note that unlike audio, Avaya Communication Manger’s bandwidth management feature does not take into account the variable video headers. Allow 20% overheads. Best practice recommends video applications should consume no more than 35% of the total WAN bandwidth.

Question 11: Is video station administration correct in the station form?

First refer to this guide or the quick setup guide.

Ensure “IP Video?” is **yes**.

Ensure “IP Video Softphone?” is **yes**.

On page 2, ensure “Direct IP-IP Audio Connections?” is **yes**.

- ☐ **Yes.**
- ☐ **No.** Expect audio only calls.

Question 12: Is signaling group administration appropriate for video support?

Review the signaling groups used between Avaya Communication Manager systems, to Polycom MGCs/RMXs, and to PathNavigators. Also refer to this guide or the quick setup guide.

Ensure “IP Video?” is **yes**.

Ensure “Direct IP-IP Audio Connections?” is **yes**.

Ensure “Calls Share IP Signaling Connection?” is **No**, though this setting may be **Yes** between Avaya Communication Manager systems.

Does the network-region value correspond to an ip-codec-set that supports video?

- ☐ **Yes**.
- ☐ **No**. Expect audio only calls.

Question 13: Does the network-region value in the change signaling-group form correspond to an ip-codec-set that supports video?

- ☐ **Yes**.
- ☐ **No**. Expect audio only calls.

Question 14: Is DSCP tagging provisioned correctly?

Ensure that DSCP parameters are provisioned for the network region to which endpoints are registered.

For Avaya Communication Manager Release 4.0: Polycom VSX 8.5.3 onwards and Polycom MGC 8.0.1 onwards will automatically obtain DSCP parameters as configured in the network region. All other endpoints should have DSCP parameters set manually to the same values to which Avaya Communication Manager is set.

- ☐ **Yes**.
- ☐ **No**. This is not best practice.

Question 15: For shared control of IP sets, is the network region of the Avaya IP Softphone the same as the IP set?

Use the **change ip-network-map** command to ensure that the Avaya IP Softphone is mapped to the same network region as the IP set.

Note:

For shared control when using video, the only option supported is **via the server**. Do not try using the **via the phone (CTI)** option.

☐ **Yes.**

☐ **No.** Do not do this. This is not supported, so expect undefined results. When using shared control with video, the network region used for Avaya IP Softphone must match the network region used by the IP set. For Avaya Communication Manager Release 5.0 and later, this will not be a limitation.

Avaya Communication Manager Administration for Ad-hoc Video Conferencing

Question 1: Are the Ad-hoc conferencing video capacities on system-parameters customer-options, page 2 configured correctly?

Ensure the “Maximum Administer Ad-hoc Video Conferencing Ports” is set to the number of ports available for Ad-hoc video conferencing.

- ☐ Yes.
- ☐ No.

Question 2: Has a Class of Service (COS) been assigned with “Ad-hoc Conferencing” enabled?

- ☐ Yes.
- ☐ No. Use the **change COS** command to enable Ad-hoc Video Conferencing.

Question 3: Has a video bridge been added using the add video-bridge command?

- ☐ Yes.
- ☐ No. Use the add video-bridge command to add Polycom MGC or Polycom RMX details for Ad-hoc video conferencing.

Avaya Communication Manager Administration for Polycom Multipoint Stations (VSX and HDX)

Question 1: Does each extension for a given multipoint endpoint have the same password configured on the station form?

For a multipoint station, each extension must have the same password. However, this password does not need to match the password for other multipoint stations.

☐ **Yes.**

☐ **No.** Use the **change station** command to set the “Security Code” entries to match. If these entries do not match, Avaya Communication Manager may reject registration by the station or confine it to one extension only.

Question 2: Has “Hunt-to Station” been configured to a circular hunt on the station form?

Configuring “Hunt-to Station” to a circular hunt enables Avaya Communication Manager to find the unused extension when dialing a multipoint station that is already in a call. This allows you to always call the main extension for the multipoint station.

☐ **Yes.**

☐ **No.** Use the **change station** command to set “Hunt-to Station” so that each station hunts to the next one, and the last station hunts to the first one.

Question 3: Has “Coverage” been configured on the station form?

The coverage feature has priority over the hunt-to feature and will interfere with it. The first call to the main Polycom VSX/HDX extension will succeed, but other calls will be busy (instead of hunting correctly). Setting “Station Hunt Before Coverage?” to “y” will also work but has system-wide consequences.

☐ **Yes.** Use the **change station** command and set “Coverage” to blank.

☐ **No.**

Avaya Communication Manager Administration for Polycom MGC Systems

Question 1: Polycom MGCs with multiple IP boards in conjunction with S87xx servers with multiple CLAN boards in regions require administration planning. Has this guide or the quick setup guide been used and understood?

☐ **Yes.**

☐ **No.** Complex signaling group and trunk group administration is required. Follow the rules in this guide and the quick setup guide. This solution offers a number of high availability options. CLAN board failures and IP board failures can be survivable. Incorrect administration can cause intermittent service.

Question 2: In Avaya Communication Manager Release 4.0, do signaling groups to Polycom MGCs have “Layer 3 Tests?” set to No?

☐ **Yes.**

☐ **No.** Expect signaling groups to go out of service (OOS).

Question 3: Is the outgoing trunk group to the Polycom MGC configured correctly in the change trunk-group form?

On Trunk group page 1, “Direction” must be **outgoing**.

On Trunk group page 1, “Outgoing Display” may be **y**. This is helpful for diagnostics.

On Trunk group page 2, “Disconnect Supervision – Out?” must be **y** to allow transfer to the MGC.

On Trunk group page 3, “Send Calling Number” must be set to allow the MGC to resolve calling party against the participant list on MGC conferences when pre-administered with participants.

☐ **Yes.**

☐ **No.** Expect trunk transfer failure. Expect wasted resources on the MGC.

Question 4: Is the incoming trunk group for the Polycom MGC configured correctly in the change trunk-group form?

On Trunk group page 1, "Direction" must be **incoming**.

On Trunk group page 2, "Disconnect Supervision – In?" must be **y** to allow transfer of MGC-initiated calls to other trunks.

- ☐ **Yes.**
- ☐ **No.** Expect trunk transfer failure.

Question 5: Is there only one incoming trunk group per Polycom MGC?

- ☐ **Yes.**
- ☐ **No.** Read this guide or the quick setup guide.

Question 6: Does the Polycom MGC have additional IP boards?

- ☐ **Yes.** For board redundancy, administer a second outgoing trunk group for the second to "nth" IP boards.
- ☐ **No.** Only one outgoing trunk group is required.

Question 7: Is the outgoing signaling group to the MGC configured correctly?

"LRQ Required?" must be **y**.

"Near end Listen Port" must be **1719**.

"Far end Listen Port" must be **1719**.

"Trunk Group for Channel Selection" must be clear.

- ☐ **Yes.**
- ☐ **No.** Expect call failures or intermittent call failures, or shuffling that shuts down video.

Question 8: Is the incoming signaling group to the Polycom MGC configured correctly?

“RRQ Required?” must be **y**.

“ARQ Required?” must be **y**.

“Near end Listen Port” must be **1720**.

“Far end Listen Port” must be **1720**.

“Trunk Group for Channel Selection” must be set to the trunk that uses the group.

☐ **Yes.**

☐ **No.** Expect call failures.

Question 9: If a Polycom MGC is to be used for six-party Ad-hoc video conferencing with Avaya Communication Manager Release 5.0, has the MGC been placed in a dedicated network region?

You must have:

- a dedicated network region for MGC use
- dedicated codec sets to infer the conference bit rates

Map the MGC to the new dedicated network region using the region field on the signaling groups connected to the MGC.

Ensure that you are using a codec set that reflects the correct conference bit rates for the MGC's network region.

Use the **change ip-network region** command to ensure that all other network regions have direct connectivity to the MGC's network region.

☐ **Yes.**

☐ **No.** Expect the MCU selection algorithms to make compromised decisions based on potentially incorrect inferred information from the codec-set conference bit rates.

Avaya Communication Manager Administration for Polycom RMX Systems

Question 1: Is a single, dual-direction trunk-group to the Polycom RMX configured correctly in the change trunk-group form?

On Trunk group page 1, “Direction” must be **both**.

On Trunk group page 1, “Outgoing Display” may be **y**. This is helpful for diagnostics.

On Trunk group page 2, “Disconnect Supervision – In?” must be **y** to allow transfer to the RMX.

On Trunk group page 2, “Disconnect Supervision – Out?” must be **y** to allow transfer to the RMX.

On Trunk group page 3, “Send Calling Number” must be set to allow the RMX to resolve calling party against the participant list on RMX conferences when pre-administered with participants.

☐ **Yes.**

☐ **No.** Expect trunk transfer failure. Expect wasted resources on the RMX.

Question 2: Is the signaling group to the Polycom RMX configured correctly?

“RRQ Required?” must be **y**.

“ARQ Required?” must be **y**.

“Near end Listen Port” must be **1720**.

“Far end Listen Port” must be **1720**.

“Trunk Group for Channel Selection” must be set to the trunk that uses the group.

☐ **Yes.**

☐ **No.** Expect call failures.

Question 3: In Avaya Communication Manager Release 4.x, do signaling groups to Polycom RMX have “Layer 3 Tests?” set to No?

☐ **Yes.**

☐ **No.** Expect signaling groups to go out of service (OOS).

Polycom MGC Configuration

Question 1: Does Network Service Properties have AVF?

Check that “Service Mode” is set to **Pseudo Gatekeeper – AVF** on the “Network Services Properties” H.323 tab.

- ☐ **Yes.**
- ☐ **No.** If this option is not available, install the Avaya version of the Polycom MGC Manager.

Question 2: Is H.245 tunneling enabled in the system.cfg file?

Check that **IP_BOARD_PARAMETERS H245_TUNNELING** is set to **YES** in the system.cfg file.

- ☐ **Yes.**
- ☐ **No.** Set this parameter to **YES**.

Question 3: Is G.729 disabled in the system.cfg file?

Check that **IP_AUDIO G729** is set to **NO** in the system.cfg file.

- ☐ **Yes.**
- ☐ **No.** You must set this parameter to **NO** to avoid call drops.

Question 4: Is wideband audio enabled in the system.cfg file?

In the system.cfg file, ensure that **AUDIO_PLUS_FREQUENCY** is set to **WB** (wideband).
NOTE: The default value for this parameter is **MB** (medium band).

- ☐ **Yes.**
- ☐ **No.** Expect no wideband support by the MGC.

Question 5: For Polycom MGC version 8, is the Avaya mode enabled in the option flag in the system.cfg file?

- ☐ **Yes.**
- ☐ **No.** You must enable this parameter.

Question 6: Is the Polycom MGC registration refresh rate set to less than 60 seconds? (35 seconds is recommended.)

☐ **Yes.**

☐ **No.** In the MGC Manager, go to **<MGC name>MCU Configuration-Network Services-IP-<service name>**. Find the H.323 tab, and ensure that “Refresh H.323 Registrations Every” is enabled and set to 35 seconds.

Question 7: Has 1*1 transcoding been set up?

Modify the desired conference room properties, and select the display option **1** on the Video Sources tab.

☐ **Yes.**

☐ **No.** MGC-MGC and MGC-RMX conference cascading may not display as expected.

Polycom RMX Configuration

Question 1: Is the Polycom RMX licensed for Avaya use?

Using the Polycom RMX web interface, go to **Administration>License Information**, and verify that Avaya is selected in “Polycom Partners.”

- ☐ **Yes.**
- ☐ **No.** Expect registration failure.

Question 2: Has the Polycom RMX system configuration been modified for use in the Avaya environment?

Using Setup menu>"System Configuration" tab, modify the following system configuration parameters:

- **MCMS_PARAMETERS:**
 - ENABLE_AUTO_EXTENSION = YES
 - MCU_DISPLAY_NAME = POLYCOM RMX-2000
 - CP_REGARD_TO_INCOMING_SETUP_RATE = NO
 - H323_FREE_VIDEO_RESOURCES = NO
 - NUMERIC_CONF_ID_LEN = 5
 - NUMERIC_CONF_ID_MAX_LEN = 8
 - NUMERIC_CONF_ID_MIN_LEN = 4
 - TERMINATE_CONF_AFTER_CHAIR_DROPPED = NO
- **CS_MODULE_PARAMETERS:**
 - H245_TUNNELING = YES

- ☐ **Yes.**
- ☐ **No.** Configuration not supported.

Question 3: Has a silence .wav file been installed?

Create a silence .wav file.

From the Polycom RMX web interface, click the note button (the right-most icon located below ivr services), and replace the music file with the silence .wav file you created.

☐ **Yes.**

☐ **No.** The RMX IVR audio for conference entry will be played when the first party joins the ad-hoc video conference.

Question 4: Has 1*1 transcoding been set up?

Modify the desired conference room properties, and select the display option **1** on the Video Sources tab.

☐ **Yes.**

☐ **No.** MGC-MGC and MGC-RMX conference cascading may not display as expected.

Polycom VSX System Configuration

Question 1: Are firewalls present between the Polycom VSX/HDX and the Avaya Communication Manager system?

- ☐ **Yes.** Ensure H.245 port range 59000-59200 is open.
- ☐ **No.**

Question 2: Does the Polycom VSX Options page have “Multipoint” or “Multipoint Trial” enabled?

- ☐ **Yes.** On the Avaya Communication Manager system, ensure that **x** (where **x** depends on the VSX type) consecutive stations are administered with the same password in a circular station hunt group. Refer to this guide or the quick setup guide.
- ☐ **No.**

Question 3: Is the “Avaya option” enabled on the Polycom VSX Options page?

- ☐ **Yes.**
- ☐ **No.** Install the new options key that will enable Avaya options.

Question 4: If H.239 is desired, is the H.239 option field enabled?

On VSX System->Admin Settings->Network->Call Preference, set **Enable H_239**.

- ☐ **Yes.**
- ☐ **No.** Dual video (people and content) will not work.

Avaya IP Softphone (IPSP)

Question 1: Did you install the USB camera with the latest drivers and verify that the camera is working?

Verify the camera works using the software that was installed with the camera (for example, use Logitech QuickCapture for Logitech cameras).

☐ **Yes.**

☐ **No.**

☐ **Question 2: Did you update the PC with the latest software?**

This is required for best performance. This includes video card drivers (VGA drivers) and Microsoft DirectX.

☐ **Yes.**

☐ **No.** Expect flickering video.

Question 3: Did you install the Avaya IP Softphone version that supports video?

Check www.avaya.com/support for the latest video Avaya IP Softphone release. Verify that the Avaya Communication Manager license supports this version of Avaya IP Softphone.

☐ **Yes.**

☐ **No.** Expect audio-only.

Question 4: Did you configure the Avaya IP Softphone Login settings for video?

Configuration:

Road Warrior

Control of Avaya Telephone (via the server)

Bandwidth Settings:

Local Area Network

Cable, xDSL or ISDN

☐ **Yes.**

☐ **No.** Video is **NOT** available with the following Settings:

Control of Avaya Telephone (via the telephone)

Telecommuter

Instant Messaging Only

28800bsp or faster modem

Question 5: Did you verify video registration after logging into Avaya IP Softphone?

Verify that the local video window opens properly.

Check the video status icon in the Avaya IP Softphone window:



Indicates that Avaya IP Softphone is not registered with video.



Indicates that Avaya IP Softphone is successfully registered with video.

☐ **Yes.**

☐ **No.** Check the Login settings in Avaya IP Softphone. (See Question 4 in this section.)
Check Video Options and manually select the camera.

Question 6: Is the Video Options outgoing call rate set to “Maximum”?

Ensure that the Video Options outgoing call rate is not set lower than the Polycom MGC/RMX conference requirements. It should only be changed from “Maximum” for specific reasons by advanced users. Avaya Communication Manager determines the call rates automatically.

☐ **Yes.**

☐ **No.** Change the Video Options outgoing call rate to meet the Polycom MGC/RMX conference requirements.

Avaya IP Softphone Performance Issues

Question 1: Are there video issues?

Check the Video Properties dialog box. Check the information on all the tabs in the dialog box.

Status – The current stats of the video.

Capabilities – The codec sets that Avaya IP Softphone currently supports.

Signaling – The current signaling with the Avaya Communication Manager system.

☐ **Yes.**

☐ **No.**

Question 2: Is Avaya IP Softphone non-responsive?

☐ **Yes.** Set the virus scanner to exclude the Avaya IP Softphone directory. See www.support.avaya.com for more information.

☐ **No.**

Question 3: If there are video issues, have you provided log files?

Logs files are located in:

C:\Program Files\Avaya\Avaya IP Softphone\Log Files*

C:\Program Files\Polycom\video\via\Video.vg2

Zip up these files and send to support.

☐ **Yes.**

☐ **No.**

Priority Bandwidth Management

Question 1: Has a COS been assigned with “Priority IP Video” enabled?

- ☐ **Yes.**
- ☐ **No.** Use **change cos** and enable **Priority IP Video**.

Question 2: Have inter-region video limits been set for normal and priority callers?

- ☐ **Yes.**
- ☐ **No.** Use **change ip-network-region** and allocate priority video bandwidth across WANs on page 3 of the form.

Question 3: Has the Maximum Call Rate for Priority Direct-IP Multimedia been set?

- ☐ **Yes.**
- ☐ **No.** Use **change ip-codec-set** and set appropriate the maximum call rates for priority and normal video users on page 2 of the form.

Question 4: Do Polycom MGC trunks need access to priority bandwidth pools across the Avaya Communication Manager network for MGC dialout scenarios?

- ☐ **Yes.** Set the “Priority Video” field to **yes** on the MGC signaling groups.
- ☐ **No.**

SIP Administration (Global)

Question 1: Is Avaya Communication Manager licensed for SIP video?

Verify that the fields have been configured correctly on page 4 of the system-parameters customer-options form. "Multimedia IP SIP Trunking?" must be set to "y."

☐ **Yes.**

☐ **No.** SIP video calls are not possible without the correct license. Installation of the license will enable the "IP Video" field on the SIP signaling group form.

Question 2: Are the video capacities configured appropriately on the system-parameters customer-options form, page 2?

"Maximum Video Capable Stations" should be equal to one time the number of single point VSX and/or three times the number of multipoint VSX and should include SIP video users.

☐ **Yes.**

☐ **No.** SIP video users are included in the total. If the limit has been reached, there will be no video calls.

Question 3: Is the authoritative domain for the IP network region in use set to match the SIP domain configured on the Avaya SIP Enablement Services (SES) server?

"Authoritative Domain" on page 1 of the ip-network-region form should be set to **yoursipdomain.com**.

☐ **Yes.**

☐ **No.** Expect "403 forbidden" denial messages, preventing call setup.

SIP Trunk Administration

Question 1: Is the SIP signaling group in use configured to allow video calls?

Verify that the fields have been configured correctly on page 1 of the signaling-group form. "IP Video?" must be set to "y."

- ☐ **Yes.**
- ☐ **No.** Video calls be audio only if a signaling group is used without IP Video allowed.

Question 2: Is the SIP signaling group configured to allow direct IP connections?

Verify that the fields have been configured correctly on page 1 of the signaling-group form. "Direct IP-IP Audio Connections?" must be set to "y."

- ☐ **Yes.**
- ☐ **No.** Video calls will be auto only if a signaling group is used without IP Video allowed.

SIP Station Administration (OPTIM)

Question 1: Is the IP station configured to use video?

Verify that the fields have been configured correctly on page 1 of the station form. "IP Video?" must be set to "y."

- ☐ **Yes.**
- ☐ **No.** Expect no video media if video is disabled for the station.

Question 2: Is the IP station configured to use direct media?

Verify that the fields have been configured correctly on page 2 of the station form. "Direct IP-IP Audio Connections?" must be set to "y."

- ☐ **Yes.**
- ☐ **No.** Expect no video media if direct media is disabled for a station.

Question 3: Is the station type correct for the SIP endpoint being administered?

Verify that the fields have been configured correctly on page 1 of the station form. "Type" must be set to "4620SIP" or "96xx."

For Avaya endpoints, ensure that the set type matches. All OPTIM video endpoints should use the "4620SIP" station type.

- ☐ **Yes.**
- ☐ **No.** An incorrect set type can cause registration failure or call setup failure.

Question 4: Is the OPTIM call limit configured to allow the number of simultaneous call appearances required by the endpoint?

Verify that the fields have been configured correctly on page 2 of the off-pbx-telephone station-mapping form. "Call Limit" should be set to the number of extensions/line appearances.

- ☐ **Yes.**
- ☐ **No.** Certain station features may be unavailable, or multipoint capabilities may not work as expected.

SIP Limitations

Question 1: In a mixed H.323/SIP environment, are all H.323 MCUs the supported RMX platform?

Verify that all H.323 bridges accessible to SIP video users are not MGCs.

☐ **Yes.**

☐ **No.** SIP video users will not receive video when dialing into an H.323 MGC. Upgrading to the Polycom RMX bridge will enable video for SIP users.

Question 2: Is the video routing feature set to prefer only H.323 trunks and not use SIP trunks with a multimedia bearer capability?

Verify that all route patterns containing SIP video trunks do not rely on the multimedia bearer capability being set.

☐ **Yes.**

☐ **No.** Multimedia bearer capability is not set for SIP video calls. As a result, SIP video calls will route as audio only.

Question 3: Is priority video enabled on a SIP signaling group, and is the bandwidth allocated from the priority pool as expected?

Verify that the signaling groups at either end of the SIP trunk have priority video enabled if it desired to use priority bandwidth. Separate sub-domain names may be used to separate priority and normal users.

☐ **Yes.**

☐ **No.** SIP currently has no means to signal a priority video call over a trunk. A system that receives a call on a priority trunk will always be allocated bandwidth from the priority pool.

Chapter 3: Setting Up Video Endpoints

This chapter describes how to

- install and configure the following video endpoints
 - Avaya IP Softphone Release 6.0 and Video Integrator
 - Polycom HDX series video conferencing system
 - Polycom VSX series video conferencing system with Release 8.5.3 or later
 - Polycom V500/V700 video calling system
 - Polycom RMX series video conferencing bridge platform
 - Polycom MGC video conferencing bridge platform with Release 8.0.0.27
 - Avaya Meeting Exchange 5.0.1 S6800 bridge
 - Polycom PathNavigator/SE200 gatekeeper
- configure Ad-hoc video conferencing on a system running Avaya Communication Manager Release 5.0
- configure a Polycom MGC video conferencing bridge platform as an H.320 gateway
- configure video trunks between two systems running Avaya Communication Manager Release 4.0 for later
- monitor the status of video bandwidth usage

Required Administration

Before administering any video endpoints on your system, you must perform the following procedures:

- configure IP codec sets
- configure IP network regions

Configure IP Codec Sets

To configure the IP codec sets that you want to use for video:

1. Use the **change ip-codec-set x** command (where **x** is the chosen IP codec set) to access the IP Codec Set form.
2. Define the codecs. The following codecs are recommended:
 - SIREN14-48K (1 fpp, 20 ms)
SIREN14-48K are wideband codecs. Since most Polycom systems are not configured for stereo, it is not recommended to use a stereo SIREN codec as a default.
 - G.722-64K (2fpp, 20 ms)
G.722-64K are wideband codecs. These codecs allow wideband with video endpoints that do not support SIREN codecs. G.722-64K codecs are required if you are using VSX systems in mixed H.320/H.323 environments. Be sure to place this codec above the other non-Siren audio codecs.
 - G.722.1-32K (1 fpp, 20 ms)
G.722.1-32K are wideband codecs. These codecs allow wideband with video endpoints that do not support SIREN codecs.
 - G.729A (no silence suppression, 2 fpp, 20 ms)
Polycom systems do not support all variants of G.729 codecs. If you want to use G.729, you must specify G.729A. If you specify G.729, no audio problems arise. All variants of G.729 codecs are narrowband codecs.

Note:

Keep in mind the following information:

- Wideband codecs should appear before narrowband codecs in the codec set. If you are using VSX systems in mixed H.320/H.323 environments, place the **G.722-64K** audio codec above the other non-Siren audio codecs.
- G.711 codecs are recommended for Avaya Meeting Exchange 5.0.1. Avaya Meeting Exchange 5.0.1 does not support wideband codecs.

3. Go to page 2 of the form.

Figure 1: Example of Page 2 of the IP Codec Set Form

IP Codec Set		
Allow Direct-IP Multimedia? <input checked="" type="checkbox"/>		
Maximum Call Rate for Direct-IP Multimedia: 1928 Kbits		
Maximum Call Rate for Priority Direct-IP Multimedia: 1928 Kbits		
	Mode	Redundancy
FAX	relay	0
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

4. Set **Allow Direct-IP Multimedia** to **y**.
5. Set **Maximum Call Rate for Direct-IP Multimedia**. The range is 128 Kbits through 768 Kbits. 384 Kbits is recommended.

This setting is the combined audio and video transmit rate or receive rate for non-priority (normal) video calls. You can use this setting to limit the amount of bandwidth used for normal video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit *and* to receive audio/video.
6. Set **Maximum Call Rate for Priority Direct-IP Multimedia**. The range is 128 Kbits through 768 Kbits. 384 Kbits is recommended.

This setting is the combined audio and video transmit rate or receive rate for priority video calls. You can use this setting to limit the amount of bandwidth used for priority video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit *and* to receive audio/video.
7. Repeat Steps 1 through 6 for each IP codec set that will be used for video.

Configure IP Network Regions

To configure the IP network regions:

- 1. Use the **change ip-network-region x** command (where **x** is the chosen IP network region) to access the IP Network Region form for the specified region.

The IP Network Region form appears.

Figure 2: Example of Page 1 of the IP Network Region Form

12345678910111213141516171819

IP NETWORK REGION

Region: 3

Location: Authoritative Domain:

Name:

MEDIA PARAMETERS

Codec Set: Intra-region IP-IP Direct Audio:

UDP Port Min: Inter-region IP-IP Direct Audio:

UDP Port Max: IP Audio Hairpinning?

DIFFSERV/TOS PARAMETERS

Call Control PHB Value: RTCP Reporting Enabled?

Audio PHB Value: RTCP MONITOR SERVER PARAMETERS

Video PHB Value: Use Default Server Parameters?

802.1P/Q PARAMETERS

Call Control 802.1p Priority:

Audio 802.1p Priority:

Video 802.1p Priority: AUDIO RESOURCE RESERVATION PARAMETERS

H.323 IP ENDPOINTS

H.323 Link Bounce Recovery?

Idle Traffic Interval (sec):

Keep-Alive Interval (sec):

Keep-Alive Count: RSUP Enabled?

- 2. Set **Intra-region IP-IP Direct Audio** to **yes**.
- 3. Set **Inter-region IP-IP Direct Audio** to **yes**.

Note:

Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

- 4. Go to page 2 of the form.

Figure 3: Example of Page 2 of the IP Network Region Form

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----

IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY

Incoming LDN Extension:

Conversion To Full Public Number - Delete: ☐ Insert:

Maximum Number of Trunks to Use for IGAR:

Dial Plan Transparency in Survivable Mode? ☒

BACKUP SERVERS(IN PRIORITY ORDER)	H.323 SECURITY PROFILES
1 <input type="text"/>	1 <input type="text" value="any-auth"/>
2 <input type="text"/>	2 <input type="text"/>
3 <input type="text"/>	3 <input type="text"/>
4 <input type="text"/>	4 <input type="text"/>
5 <input type="text"/>	
6 <input type="text"/>	

Allow SIP URI Conversion? ☒

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS

Near End Establishes TCP Signaling Socket? ☒

Near End TCP Port Min:

Near End TCP Port Max:

5. Set **Security Procedures 1** to **any-auth**.
6. Go to page 3 of the form.

Figure 4: Example of Page 3 of the IP Network Region Form

Inter Network Region Connection Management																		
src rgn	dst rgn	codec set	direct WAN	Total WAN-BW-limits	Video Norm	Prio	Shr	Intervening-regions	Dyn CAC	IGAR								
2	1	2	y	384 Kbits	0	0	y			n								
2	2	2																
2	3	2	n					4: 1: :		n								
2	4	4	y	: NoLimit	4294		n			n								
2	5	5	y	10 Mbits	0	0	y			n								
2	6	4	n					4: 1: 3: 7		n								
2	7																	
2	8																	
2	9																	
2	10																	
2	11																	
2	12																	
2	13																	
2	14																	
2	15																	

7. Set **codec set** to the codec set you defined in Procedure 2.
8. Set **Video Norm** to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
9. Set **Video Prio** to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
10. Set **Video Shr**. Specify whether the normal video pool can be shared with the audio pool for each link between IP network regions (**y** or **n**).
11. Repeat Steps 1 through 10 for each IP network region that will be used for video in this system.

Configure a Station Endpoint for Avaya IP Softphone Release 6.0 and Video Integrator

This section describes how to enable video calls for a desktop user.

Note:

Users must install Avaya IP Softphone Release 6.0 and Video Integrator on their PCs before they can handle video calls from their desktops.

Checklist

When setting up video calls for a desktop, you will need to know the following information:

- the station number of the desktop user
- the IP codec sets you want to use
- the IP network regions you want use

Configuration Procedures

To configure a station to use Avaya IP Softphone R6.0 and Video Integrator, you must perform the following steps:

1. Determine the maximum number of video-capable Avaya IP Softphone endpoints your voice system supports.
2. Configure the Class of Service if you want to use priority video calling.
3. Add a new station or modify an existing station that will use Avaya IP Softphone for video.

Procedure 1: Determine the Maximum Number of Video-Capable Avaya IP Softphone Endpoints Supported

To determine the maximum number of video-capable Avaya IP Softphone endpoints your voice system supports:

- 1. Use the **display system-parameters customer-options** command to access the Optional Features form.
- 2. On page 2 of the form, verify the **Maximum Video Capable IP Softphones**. This number is provided by the RFA license file.

Note:
To provide video softphone capability, you must have at least this number of IP Softphone licenses. Page 10 of this form displays the number of IP Softphone licenses you have.

Figure 5: Example of Page 2 of the Optional Features Form

12345678910

OPTIONAL FEATURES

IP PORT CAPACITIES

Maximum Administered H.323 Trunks: 200

Maximum Concurrently Registered IP Stations: 40

Maximum Administered Remote Office Trunks: 0

Maximum Concurrently Registered Remote Office Stations: 0

Maximum Concurrently Registered IP eCons: 10

Max Concur Registered Unauthenticated H.323 Stations: 10

Maximum Video Capable Stations: 40

Maximum Video Capable IP Softphones: 40

Maximum Administered SIP Trunks: 100

Maximum Administered Ad-hoc Video Conferencing Ports: 217

Maximum Number of DS1 Boards with Echo Cancellation: 0

Maximum TN2501 VAL Boards: 0

Maximum Media Gateway VAL Sources: 0

Maximum TN2602 Boards with 80 VoIP Channels: 0

Maximum TN2602 Boards with 320 VoIP Channels: 0

Maximum Number of Expanded Meet-me Conference Ports: 0

USED

174

7

0

0

0

0

20

14

70

100

0

0

0

0

0

(NOTE: You must logoff & login to effect the permission changes.)

In this example, the system can have a maximum of 40 video-enabled Avaya IP Softphones. Currently, 14 video-capable Avaya IP Softphones are being used.

Procedure 2: Configure Class of Service

Perform this procedure if you want to allow priority video calling.

To configure the Class of Service:

1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.

Figure 6: Example of Page 2 of the Class of Service Form

1 2		CLASS OF SERVICE															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
VIP Caller		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Masking CPN/Name Override		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Call Forwarding Enhanced		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Priority Ip Video		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ad-hoc Video Conferencing		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Set **Priority Video Calling** for the appropriate COS levels.

Procedure 3: Add a Video-Enabled Avaya IP Softphone Station

To add a video-enabled Avaya IP Softphone station:

1. Perform one of the following steps:

- If you want to add a new station that will use Avaya IP Softphone, use the **add station** command.
- If you want to modify an existing station that will use Avaya IP Softphone, use the **change station xxxx** (where **xxxx** is the number of the station you want to modify) command.

The Station form appears.

Figure 7: Example of Page 1 of the Station Form

1	2	3	4	5
STATION				
Extension:	3000	Lock Messages?	<input type="checkbox"/>	BCC:
Type:	6408D+	Security Code:	<input type="text"/>	TN:
Port:	<input type="text"/>	Coverage Path 1:	<input type="text"/>	COR:
Name:	<input type="text"/>	Coverage Path 2:	<input type="text"/>	COS:
		Hunt-to Station:	<input type="text"/>	
STATION OPTIONS				
Loss Group:	2	Time of Day Lock Table:	<input type="text"/>	
Data Module?	<input type="checkbox"/>	Personalized Ringing Pattern:	<input type="text"/>	
Speakerphone:	2-way	Message Lamp Ext:	3000	
Display Language:	english	Mute Button Enabled?	<input type="checkbox"/>	
Survivable COR:	internal	Media Complex Ext:	<input type="text"/>	
Survivable Trunk Dest?	<input type="checkbox"/>	IP SoftPhone?	<input type="checkbox"/>	
		IP Video?	<input type="checkbox"/>	

2. Enter the appropriate information for this station.
3. Set **IP Softphone** to **y**.
4. Set **IP Video Softphone** to **y**.
5. If you want this station to be able to make priority video calls, make sure you select a COS level that has **Priority Video Calling** enabled. (See Procedure 2.)
6. Repeat Steps 1 through 5 for each video-enabled Avaya IP Softphone endpoint you want to configure.

Configure Polycom VSX/HDX Series Video Conferencing Systems and V500/V700 Video Calling Systems

Use this procedure to configure Polycom VSX/HDX series video conferencing systems and V500 and V700 video calling systems.

Checklist

When setting up these systems, you will need to know the following information:

- maximum number of VSX/HDX, V500, and V700 systems on your network
- PIN for each VSX/V500/V700 system. The PIN can consist of a maximum of eight numeric characters and is defined by the System Administrator.
- the key code that combines the Avaya option with any other Polycom options.
- whether the VSX/HDX system has the multipoint option or IMCU option. If so, you must combine the Polycom Software License for this capability with the “Avaya Option” Polycom Software License to create a single Key Code to input into the unit.
- IP address of the voice system
- the IP codec sets you want to use
- the IP network regions you want use

Configuration Procedures

To configure Polycom VSX/HDX series video conferencing systems and V500/V700 video calling systems, you must perform the following steps:

1. Determine the maximum number of video-capable H.323 stations your voice system supports.
2. Configure the Class of Service if you want to use priority video calling.
3. Add a new station for the Polycom system.
4. Configure the Polycom system.

Procedure 1: Determine the Maximum Number of Video-Capable H.323 Stations Supported

To determine the maximum number of video-capable H.323 endpoints your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the **Maximum Video Capable Stations**. This number is provided by the RFA license file. The **Maximum Video Capable Stations** was determined using the following criteria:
 - Each V500/V700 system is considered to be **one** station.
 - Each single-point VSX system is considered to be **one** station.
 - Each VSX multipoint system can be **three** to **six** stations.
 - Each HDX system can be three stations for multipoint plus four and seven for multipoint plus eight multipoint licensed options for the HDX9004. The HDX9002 only has multipoint plus 4 as an option.

Figure 8: Example of Page 2 of the Optional Features Form

1	2	3	4	5	6	7	8	9	10
OPTIONAL FEATURES									
IP PORT CAPACITIES									
Maximum Administered H.323 Trunks: 200									USED 174
Maximum Concurrently Registered IP Stations: 40									7
Maximum Administered Remote Office Trunks: 0									0
Maximum Concurrently Registered Remote Office Stations: 0									0
Maximum Concurrently Registered IP eCons: 10									0
Max Concur Registered Unauthenticated H.323 Stations: 10									0
Maximum Video Capable Stations: 40									20
Maximum Video Capable IP Softphones: 40									14
Maximum Administered SIP Trunks: 100									70
Maximum Administered Ad-hoc Video Conferencing Ports: 217									100
Maximum Number of DS1 Boards with Echo Cancellation: 0									0
Maximum TN2501 VAL Boards: 0									0
Maximum Media Gateway VAL Sources: 0									0
Maximum TN2602 Boards with 80 VoIP Channels: 0									0
Maximum TN2602 Boards with 320 VoIP Channels: 0									0
Maximum Number of Expanded Meet-me Conference Ports: 0									0
(NOTE: You must logoff & login to effect the permission changes.)									

In this example, the system can have a maximum of 40 video-capable stations. Currently, 20 video-capable H.323 stations are being used.

Procedure 2: Configure Class of Service

Perform this procedure if you want to allow priority video calling.

To configure the Class of Service:

- 1. Use the **change cos** command to access the Class of Service form.
- 2. Go to page 2 of the form.

Figure 9: Example of Page 2 of the Class of Service Form

12

CLASS OF SERVICE

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
VIP Caller	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Masking CPN/Name Override	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Call Forwarding Enhanced	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Priority Ip Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ad-hoc Video Conferencing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- 3. Set **Priority Video Calling** for the appropriate COS levels.

Procedure 3: Add a Station for the Polycom System

To add a station:

1. Use the **add station** command.

The Station form appears.

Figure 10: Example of Page 1 of the Station Form

1	2	3	4
STATION			
Extension: 71280	Lock Messages? <input type="checkbox"/>	BCC: 0	
Type: <input type="text" value="H.323"/>	Security Code: <input type="text" value="*"/>	TN: <input type="text" value="1"/>	
Port: S000008	Coverage Path 1: <input type="text"/>	COR: <input type="text" value="1"/>	
Name: VSX 8000 #1	Coverage Path 2: <input type="text"/>	COS: <input type="text" value="1"/>	
	Hunt-to Station: <input type="text" value="71281"/>	Tests? <input type="checkbox"/>	
STATION OPTIONS			
Loss Group: <input type="text" value="19"/>	Time of Day Lock Table: <input type="text"/>	Message Waiting Indicator: <input type="text" value="none"/>	
Survivable COR: <input type="text" value="internal"/>	IP Video? <input type="checkbox"/>		
Survivable Trunk Dest? <input type="checkbox"/>			
DTMF over IP: <input type="text" value="in-band"/>			

2. Enter the appropriate information for this station.
3. Set **Type** to **H.323**.
4. Set **Security Code** to the “pin” you will administer for the VSXHDX or V500 system.
5. Set **IP Video** to **y**.
6. If you want this station to be able to make priority video calls, make sure you select a COS level that has **Priority Video Calling** enabled. (See Procedure 2.)

Note:

You can create an alias for VSX/HDX stations.

Setting Up Video Endpoints

7. If the VSX system has the multipoint option or IMCU option, perform the following steps:
 - a. Use the **add station** command to add a second station for the Polycom system.
 - b. Set **Type** to **H.323**.
 - c. Set **Security Code** to the “pin” you will administer for the VSX/HDX. Make sure the security code is the same as the previous station. All three stations must have the same security code.
 - d. Set **IP Video** to **y**.
 - e. Go to page 2 of the form.

Figure 11: Example of Page 2 of the Station Form

1	2	3	4
STATION			
FEATURE OPTIONS			
LWC Reception: <input type="text" value="spe"/>			
LWC Activation? <input type="checkbox" value="y"/>		Coverage Msg Retrieval? <input type="checkbox" value="y"/>	
LWC Log External Calls? <input type="checkbox" value="n"/>			
CDR Privacy? <input type="checkbox" value="n"/>		Data Restriction? <input type="checkbox" value="n"/>	
Redirect Notification? <input type="checkbox" value="y"/>		Call Waiting Indication: <input type="checkbox" value="y"/>	
Per Button Ring Control? <input type="checkbox" value="n"/>		Att. Call Waiting Indication: <input type="checkbox" value="y"/>	
Bridged Call Alerting? <input type="checkbox" value="n"/>			
Switchhook Flash? <input type="checkbox" value="y"/>			
H.320 Conversion? <input type="checkbox" value="n"/>		Per Station CPN - Send Calling Number? <input type="checkbox"/>	
MWI Served User Type: <input type="text"/>			
AUDIX Name: <input type="text"/>		Coverage After Forwarding? <input type="text" value="S"/>	
Emergency Location Ext: <input type="text" value="71280"/>		Direct IP-IP Audio Connections? <input type="checkbox" value="y"/>	
		IP Audio Hairpinning? <input type="checkbox" value="y"/>	

- f. Set **Direct IP-IP Audio Connections** to **y**.
- g. Set **IP Audio Hairpinning** to **y**.
- h. If you want this station to be able to make priority video calls, make sure you select a COS level that has **Priority Video Calling** enabled. (See Procedure 4.)
- i. Repeat Steps a through h to create the third consecutive station.

Note:

You can have up to six stations.

- j. Use the **change station xx** command (where **xx** is the first station you added for the Polycom system) to set **Hunt-to Station** to the second station you added for the Polycom system.
- k. Use the **change station xx** command (where **xx** is the second station you added for the Polycom system) to set **Hunt-to Station** to the third station you added for the Polycom system.
- l. Use the **change station xx** command (where **xx** is the third station you added for the Polycom system) to set **Hunt-to Station** to the first station you added for the Polycom system. All three stations must be in a circular hunt.

Note:

If you added more than three stations for the Polycom system, use the **change station xx** command to set **Hunt-to Station** for each station. All of the stations you add must be in a circular hunt.

8. Repeat Steps 1 through 7 for each Polycom system.

Procedure 4: Configure the Polycom System

To configure the Polycom system:

1. Install the Polycom system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Using a web browser, access the Polycom home page for the unit, and select **Admin Settings>Network>IP Network**.
4. Select the **Enable IP H.323** check box.
5. Select the **Display H.323 Extension** check box.
6. In the H.323 Extension (E.164) box, enter the station number you specified for this system on the Avaya Communication Manager system.
7. From the Use Gatekeeper box, select **Specify with PIN**.
8. In the Gatekeeper IP Address box, enter the IP address of the CLAN or PCLAN followed by **:1719** (to specify the correct port to use).
9. In the Authentication PIN box, enter the security code you entered in Procedure 4.
10. In the Number box in the Gateway area, enter the extension you specified.
11. Select the **Enabled PVEC** check box.
12. In the Type of Service box in the Quality of Service area, select the appropriate setting. Both **IP Precedence** and **Diffserve** are supported. Contact your Network Administrator for this information.
13. In the Type of Service Value boxes (Video, Audio, and Far End Camera Control), enter the QoS values for the IP Network Region settings in which the VSX station belongs.
14. Select the **Dynamic Bandwidth** check box.

Setting Up Video Endpoints

15. From the Maximum Transmit Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
16. From the Maximum Receive Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
17. Complete the Firewall and Streaming sections as necessary.
18. When finished, click the **Update** button.
19. Repeat Steps 1 through 18 for each Polycom system.

Configure a Polycom RMX Series Video Conferencing Bridge Platform

This section describes how to configure a Polycom RMX series video conferencing bridge platform for use with an Avaya server.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the RMX system
- the IP address of the CLAN

Note:

Make sure you have the RMX Installation and Configuration guide available when you configure the RMX.

Configuration Procedures

To configure a Polycom RMX video conferencing bridge platform, you must perform the following steps:

1. Add an entry in the IP Node Names for the RMX system.
2. Add a two-way trunk group for the RMX system.
3. Add a signaling group for the RMX system.
4. Add members to the two-way trunk group for the RMX system.
5. Create a route pattern for the trunk group.
6. Configure the RMX system.

Procedure 1: Add an Entry in the IP Node Names for the RMX System

To add an entry in the IP Node Names form for the RMX system:

- 1. Use the **change node-names ip** command to access the IP Node Names form.
- 2. In the Name field, enter a name for the RMX system.
- 3. In the corresponding IP Address field, enter the IP address of the signaling host for the RMX system.

Procedure 2: Add a Two-Way Trunk Group for the RMX System

To add a two-way trunk group for the RMX system:

- 1. Use the **add trunk-group xx** command (where **xx** is the chosen trunk group) to access the Trunk Group form.
- The Trunk Group form appears.

Figure 12: Example of Page 1 of the Trunk Group Form

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
TRUNK GROUP																				
Group Number: 54					Group Type: isdn					CDR Reports: y										
Group Name: RMX Simulator					COR: 1					TN: 1					TAC: 154					
Direction: two-way					Outgoing Display? n					Carrier Medium: H.323										
Dial Access? y					Busy Threshold: 255					Night Service:										
Queue Length: 0																				
Service Type: tie					Auth Code? n															
										Member Assignment Method: auto										
										Signaling Group: 54										
										Number of Members: 10										

- 2. Set **Group Type** to **isdn**.
- 3. Set **Direction** to **two-way**.

4. Set **Carrier Medium** to **H.323**.
5. Set **Service Type** to **tie**.

Procedure 3: Add a Signaling Group for the RMX System

To add a signaling group for the RMX system:

1. Use the **add signaling-group xx** command (where **xx** is the chosen signaling group) to access the Signaling Group form.

The Signaling Group form appears.

Figure 13: Example of Page 1 of the Signaling Group Form

1	2	3	4	5
SIGNALING GROUP				
Group Number: 54		Group Type: h.323		
Remote Office? <input type="checkbox"/>		Max number of NCA TSC: <input type="text" value="0"/>		
SBS? <input type="checkbox"/>		Max number of CA TSC: <input type="text" value="0"/>		
IP Video? <input checked="" type="checkbox"/>		Trunk Group for NCA TSC: <input type="text"/>		
Priority Video? <input type="checkbox"/>				
Trunk Group for Channel Selection: <input type="text" value="54"/>				
TSC Supplementary Service Protocol: <input type="text" value="a"/>				
T303 Timer(sec): <input type="text" value="10"/>				
Near-end Node Name: <input type="text" value="procr"/>		Far-end Node Name: <input type="text" value="rmx-sin"/>		
Near-end Listen Port: <input type="text" value="1720"/>		Far-end Listen Port: <input type="text" value="1720"/>		
LRQ Required? <input type="checkbox"/>		Far-end Network Region: <input type="text" value="1"/>		
RRQ Required? <input type="checkbox"/>		Calls Share IP Signaling Connection? <input type="checkbox"/>		
Media Encryption? <input type="checkbox"/>		Bypass If IP Threshold Exceeded? <input type="checkbox"/>		
DTMF over IP: <input type="text" value="out-of-band"/>		H.235 Annex H Required? <input type="checkbox"/>		
Link Loss Delay Timer(sec): <input type="text" value="90"/>		Direct IP-IP Audio Connections? <input checked="" type="checkbox"/>		
Enable Layer 3 Test? <input type="checkbox"/>		IP Audio Hairpinning? <input type="checkbox"/>		
		Interworking Message: <input type="text" value="PROGress"/>		
		DCP/Analog Bearer Capability: <input type="text" value="3.1kHz"/>		

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Trunk Group for Channel Selection** to the two-way trunk group you added.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter **procr**. For an S8500 or S8700 system, you would enter the name of the CLAN board.

Setting Up Video Endpoints

7. Set **Near-end Listen Port** to **1720**.
8. Set **LRQ Required** to **n**.
9. Set **RRQ Required** to **y**.
10. Set **Enable Layer 3 Test** to **n**.
11. Set **Far-end Node Name** to the name you entered for the RMX system.
12. Set **Far-end Listen Port** to **1720**.
13. Set the **Far-end Network Region**.
14. Set **Calls Share IP Signaling Connection** to **n**.
15. Set **Direct IP-IP Audio Connections** to **y**.
16. Set **IP Audio Hairpinning** to **n**.

Procedure 4: Add Members to the Two-Way Trunk Group

To add members to the two-way trunk group:

1. Use the **change trunk-group xx** command (where **xx** is the incoming trunk group you added) to access the Trunk Group form.

The Trunk Group form appears.

2. Go to page 5 of the Trunk Group form.

Page 5 of the Trunk Group form appears.

Figure 14: Example of Page 5 of the Trunk Group Form

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21		
TRUNK GROUP																						
																		Administered Members (min/max):			1/10	
																		Total Administered Members:			10	
GROUP MEMBER ASSIGNMENTS																						
Port					Name					Night												
1: T00195					RMX Simula					<input type="text"/>												
2: T00196					RMX Simula					<input type="text"/>												
3: T00197					RMX Simula					<input type="text"/>												
4: T00198					RMX Simula					<input type="text"/>												
5: T00199					RMX Simula					<input type="text"/>												
6: T00200					RMX Simula					<input type="text"/>												
7: T00201					RMX Simula					<input type="text"/>												
8: T00202					RMX Simula					<input type="text"/>												
9: T00203					RMX Simula					<input type="text"/>												
10: T00204					RMX Simula					<input type="text"/>												
11:										<input type="text"/>												
12:										<input type="text"/>												
13:										<input type="text"/>												
14:										<input type="text"/>												
15:										<input type="text"/>												

3. Add members to the trunk group. The number of members depends on the maximum simultaneous calls an RMX supports.

Procedure 5: Create a Route Pattern for the RMX Trunk Group

To create a route pattern that points to the two-way trunk group:

1. Use the **change route-pattern xx** command (where **xx** is the route pattern you want to use) to access the Route Pattern form.

The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the two-way trunk group you created for the RMX.

Procedure 6: Configure the RMX System

To configure the Polycom RMX system:

1. Install the RMX system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Access the Polycom home page for the unit.
4. From the Setup menu, select the **System Configuration** tab.
5. Under MCMS_PARAMETERS_USER, configure the following settings:
 - MCU_DISPLAY_NAME = POLYCOM RMX-2000
 - ENABLE_AUTO_EXTENSION = YES
 - NUMERIC_CONF_ID_LEN = 5
 - CP_REGARD_TO_INCOMING_SETUP_RATE = NO
 - NUMERIC_CONF_ID_MAX_LEN = 8
 - NUMERIC_CONF_ID_MIN_LEN = 4
 - TERMINATE_CONF_AFTER_CHAIR_DROP = NO
 - H323_FREE_VIDEO_RESOURCES = NO
6. Under CS_MODULE_PARAMETERS, add the following information:
H245_TUNNELING = YES
7. Create an H.323 service, and enter the CLAN IP address of the Avaya Communication Manager system as the primary gatekeeper. Confirm via a status signaling group that the RMX has registered.
8. Create a meeting room to use a test direct dial conference ID.

If you want to configure Ad-hoc conferencing for the RMX system, go to [Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform](#) on page 71.

Configure Ad-hoc Video Conferencing for a Polycom RMX Series Video Conferencing Bridge Platform

This section describes how to configure Ad-hoc video conferencing for a Polycom RMX series video conferencing bridge platform.

Checklist

When setting up Ad-hoc conferencing on a Polycom RMX system, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the RMX system
- the IP address of the CLAN

Note:

Make sure you have the RMX Installation and Configuration guide available when you configure the RMX.

Configuration Procedures

To configure Ad-hoc conferencing, you must perform the following steps:

1. Configure the RMX for use with an Avaya server.
2. Determine the maximum number of Ad-hoc video conferencing ports your voice system supports.
3. Configure the Class of Service for Ad-hoc video conferencing.
4. Configure a video bridge.
5. Configure the RMX system for Ad-hoc conferencing.

Procedure 1: Configure the Polycom RMX for Use with an Avaya Server

Perform the procedures in the section [Configure a Polycom RMX Series Video Conferencing Bridge Platform](#) on page 65 to configure the Polycom RMX system. After performing these procedures, go to [Procedure 2: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported](#) on page 72.

Procedure 2: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported

To determine the maximum number of Ad-hoc video conferencing ports your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the sum of the ports on your RMX systems. For example, if you have an RMX20 system and an RMX80 system, the maximum number of ports is 100.

Figure 15: Example of Page 2 of the Optional Features Form

1	2	3	4	5	6	7	8	9	10
OPTIONAL FEATURES									
IP PORT CAPACITIES									USED
Maximum Administered H.323 Trunks: 200									174
Maximum Concurrently Registered IP Stations: 40									7
Maximum Administered Remote Office Trunks: 0									0
Maximum Concurrently Registered Remote Office Stations: 0									0
Maximum Concurrently Registered IP eCons: 10									0
Max Concur Registered Unauthenticated H.323 Stations: 10									0
Maximum Video Capable Stations: 40									20
Maximum Video Capable IP Softphones: 40									14
Maximum Administered SIP Trunks: 100									70
Maximum Administered Ad-hoc Video Conferencing Ports: 217									100
Maximum Number of DS1 Boards with Echo Cancellation: 0									0
Maximum TN2501 VAL Boards: 0									0
Maximum Media Gateway VAL Sources: 0									0
Maximum TN2602 Boards with 80 VoIP Channels: 0									0
Maximum TN2602 Boards with 320 VoIP Channels: 0									0
Maximum Number of Expanded Meet-me Conference Ports: 0									0
(NOTE: You must logoff & login to effect the permission changes.)									

In this example, the system can have a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

Procedure 3: Configure Class of Service

To configure the Class of Service:

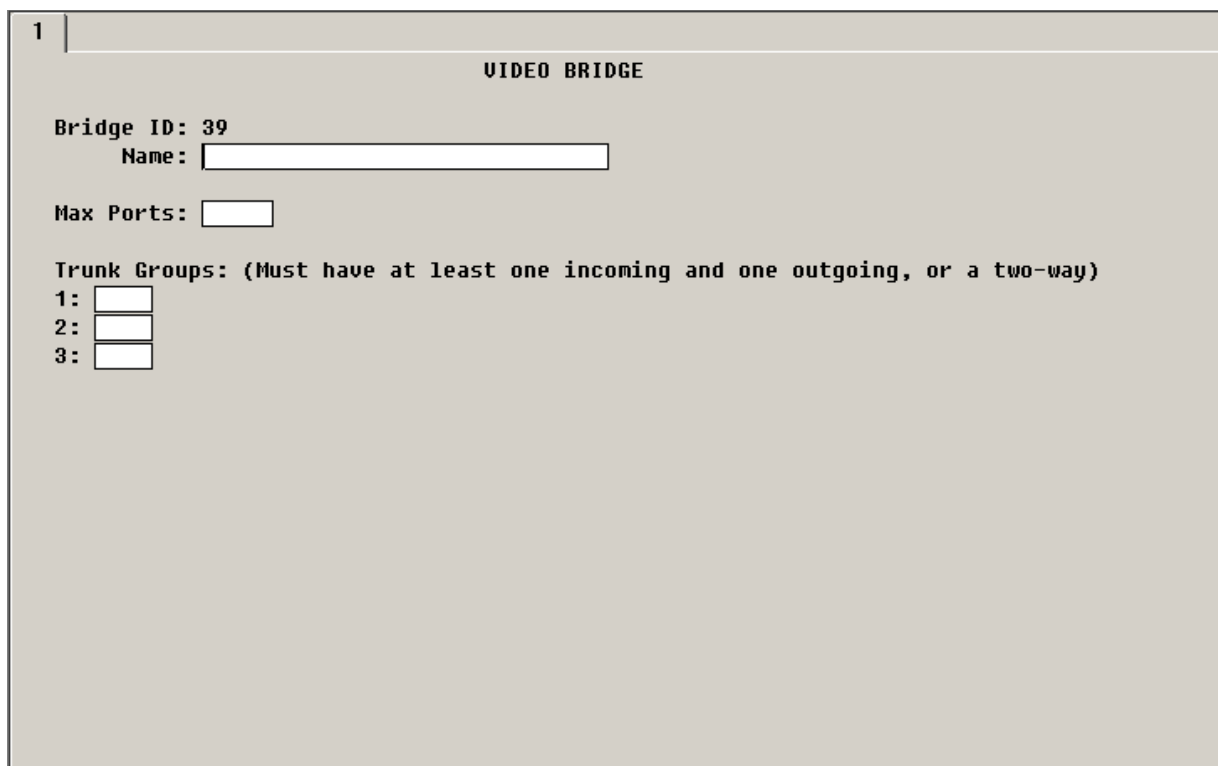
1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.

Procedure 4: Configure a Video Bridge

To configure a video bridge:

1. Use the **add video-bridge xx** command (where **xx** is the bridge number between 1 to 40) to access the Video Bridge form.

Figure 16: Example of the Video Bridge Form

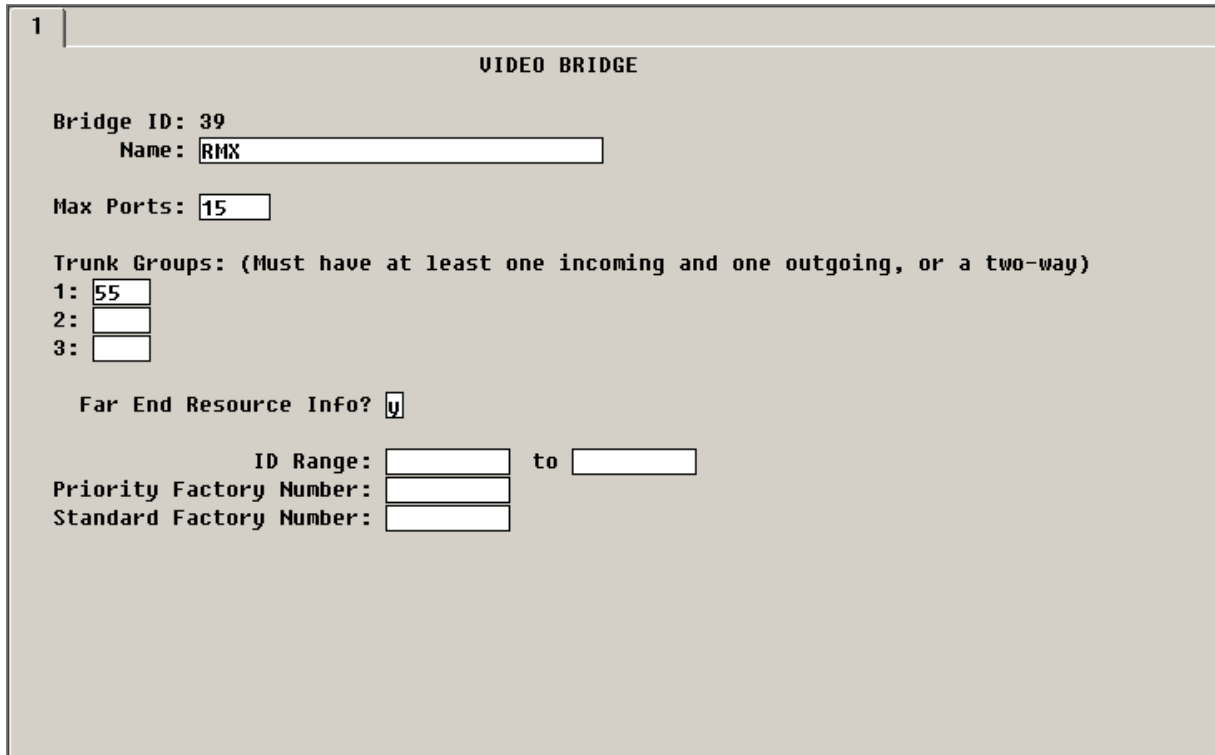


The screenshot shows a web-based configuration form titled "VIDEO BRIDGE". The form is set for "Bridge ID: 39". It includes a "Name:" field with a text input box, a "Max Ports:" field with a numeric input box, and a "Trunk Groups:" section. The trunk groups section has a header "(Must have at least one incoming and one outgoing, or a two-way)" and three rows labeled "1:", "2:", and "3:", each followed by a dropdown menu.

2. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - RMX*).
3. Set **Max Ports** to the maximum number of Ad-hoc conferencing ports you want to assign to this bridge. (The minimum you can enter is 3.) This is equivalent to the number of ports for Ad-hoc use on the associated RMX. You can use Max Ports to limit the extent of Ad-hoc usage of an RMX and thereby reserve ports for scheduled usage.
4. In **Trunk Groups**, enter the administered two-way ISDN H.323 trunk groups you added in [Procedure 2: Add a Two-Way Trunk Group for the RMX System](#) on page 66. All entries must be of the same carrier type (that is, all H.323 trunks).

The Far End Resource Info, ID Range, Priority Factory Number, and Standard Factory Number fields appear.

Figure 17: Example of the Video Bridge Form



1 | VIDEO BRIDGE

Bridge ID: 39
 Name: RMX

Max Ports: 15

Trunk Groups: (Must have at least one incoming and one outgoing, or a two-way)
 1: 55
 2:
 3:

Far End Resource Info? y

ID Range: to
 Priority Factory Number:
 Standard Factory Number:

5. Make sure **Far End Resource Info?** is set to **y**.
6. Set **ID Range** to the range of ports. The IDs you specify on this form must **NOT** be configured on the RMX. You must leave these IDs free for the factory to create its own conferences there. Note that Automatic Alternate Routing (AAR) and Unified Dial Plan (UDP) are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan. As a result, you can set up several video bridges with exactly the same conference IDs and numbers. (This will make it easier for you to maintain configurations and swap hardware.)
7. Set **Priority Factory Number**. This number represents the Entry Queue created on the RMX and corresponds to a priority conference service level (for example, 784 Kbps). The Priority Factory Number must **NEVER** be in the conference ID range.
 If this field is left blank, all conferences can use the bridge. However, priority conferences will try to find a video bridge that has a priority factory (if there is one).

8. Set **Standard Factory Number**. This number represents the Entry Queue created on the RMX and corresponds to a standard conference service level (for example, 384 Kbps). The Standard Factory Number must **NEVER** be in the conference ID range.

If this field is left blank, non-priority conferences cannot use this video bridge. A conference started by a priority user with non-priority users may be moved to a priority bridge, and the non-priority users will connect to it and receive video.

Note:

You must specify either a Priority Factory Number or a Standard Factory number.
You cannot leave both fields blank.

Procedure 5: Configure the RMX System

On the Polycom RMX system, perform the following steps for Ad-hoc conferencing:

1. Create conference profiles for Ad Hoc (and Meeting Room) style conferences.

Note:

Be sure to choose **Auto Layout** under the video settings.

2. Create the two entry queues (one for Ad-hoc conferences, and one for priority conferences).
3. For the "Conference IVR Service," perform the following steps:
 - a. Under the Welcome tab, disable the **Enable Welcome Messages** check box.
 - b. Under the Conference Chairperson tab, disable the **Chairperson messages** check box.
 - c. Under the Conference Password tab, disable the **Enable Password Messages** check box.
4. Under the General tab, perform the following steps:
 - a. Deselect any .wav file for the First to Join announcement.
 - b. Disable roll call.
 - c. Disable click and view.
5. Under the IVR Service tab, click the music icon, and set a silence .wav file as the IVR message. A silence .wav file will disable music from being played to the first party who joins the conference. To create a silence .wav file:
 - a. Open the Windows Sound Recorder application.
 - b. From the File menu, select **Save As**.

The Save As dialog box appears.
 - c. Click the **Change** button.
 - d. In the Name box, enter **silence.wav**.
 - e. From the Format box, select **PCM**.

- f. From the Attributes box, select **16.00 kHz, 16 Bit, Mono**.
- g. Click the **OK** button.

Display Capacity for Ad-hoc Video Conferencing

To display the capacity for Ad-hoc video conferencing:

1. Use the **display capacity** command to access the System Capacity form.
2. Go to page 7. Ad-hoc Video Conferencing Ports displays the following Ad-hoc video conferencing information:
 - Used - the number of video conferencing ports currently in use.
 - Available - the number of video conferencing ports currently available.
 - System Limit - the total number of video conference ports in your system. (This is the sum of Used ports and Available ports.)

View Video Conferencing Bridges

Use the **list video-bridge** command to view the video conferencing bridges administered on your system.

Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server

This section describes how to configure a Polycom MGC-25 video conferencing bridge platform for use with an Avaya S8300 server.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the MGC system
- the IP address of the CLAN

Configuration Procedures

To configure a Polycom MGC-25 video conferencing bridge platform for use with an Avaya S8300 server, you must perform the following steps:

1. Add an entry in the IP Node Names for the MGC system.
2. Add a two-way trunk group for the MGC system.
3. Add a signaling group for the MGC system.
4. Add members to the two-way trunk group for the MGC system.
5. Create a route pattern for the trunk group.
6. Configure the MGC system.

Procedure 1: Add an Entry in the IP Node Names for the MGC System

To add an entry in the IP Node Names form for the MGC system:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the **Name** field, enter a name for the MGC system.
3. In the corresponding **IP Address** field, enter the IP address of the IP board for the MGC system.

Procedure 2: Add a Two-Way Trunk Group for the MGC System

To add a two-way trunk group for the MGC system:

1. Use the **add trunk-group xx** command (where **xx** is the chosen trunk group) to access the Trunk Group form.

The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Set **Direction** to **two-way**.
4. Set **Carrier Medium** to **H.323**.
5. Set **Service Type** to **tie**.

Procedure 3: Add a Signaling Group for the MGC System

To add a signaling group for the MGC system:

1. Use the **add signaling-group xx** command (where **xx** is the chosen signaling group) to access the Signaling Group form.

The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Trunk Group for Channel Selection** to the two-way trunk group you added.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter **procr**. For an S8500 or S8700 system, you would enter the name of the CLAN board.
7. Set **Near-end Listen Port** to **1720**.
8. Set **LRQ Required** to **n**.
9. Set **RRQ Required** to **y**.
10. Set **Enable Layer 3 Test** to **n**.
11. Set **Far-end Node Name** to the name you entered for the MGC system.
12. Set **Far-end Listen Port** to **1720**.
13. Set the **Far-end Network Region**.
14. Set **Calls Share IP Signaling Connection** to **n**.
15. Set **Direct IP-IP Audio Connections** to **y**.
16. Set **IP Audio Hairpinning** to **n**.

Procedure 4: Add Members to the Two-Way Trunk Group

To add members to the two-way trunk group:

1. Use the **change trunk-group xx** command (where **xx** is the incoming trunk group you added) to access the Trunk Group form.

The Trunk Group form appears.

2. Go to page 5 of the Trunk Group form.

Page 5 of the Trunk Group form appears.

3. Add members to the trunk group.

Procedure 5: Create a Route Pattern for the MGC Trunk Group

To create a route pattern that points to the two-way trunk group:

1. Use the **change route-pattern xx** command (where **xx** is the route pattern you want to use) to access the Route Pattern form.

The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the two-way trunk group you created for the MGC.

Procedure 6: Configure the MGC System

To configure the Polycom MGC system:

1. Install the MGC system and connect it to your network.
2. Upgrade the Polycom system software (if necessary).
3. Access the Polycom home page for the unit, and select **MCU Configuration>Network Services>IP>IP Default>Network Service Properties**.
4. Create a new H.323 service.
5. On the Settings tab, perform the following steps:
 - a. Set **Protocol** to **H323**.
 - b. Specify the **Subnet Mask**.
 - c. Specify the **Default Router**.
6. On the DNS Settings tab, specify the appropriate DNS servers in the **Use DNS Servers** box.
7. On the H323 tab, perform the following steps:
 - a. Make sure the **Forwarding** check box is not enabled.
 - b. In the **Use Gatekeeper** box, specify the gatekeeper.
 - c. In the **Preferred Gatekeeper IP Address** box, enter the CLAN IP address.

- d. In the **Service Mode** box, enter **Pseudo Gatekeeper AVF**.

Note:

If **Pseudo Gatekeeper AVF** does not appear, you do not have the latest software. You must install the Avaya-enabled Polycom MGC Manager software.

- e. In the Prefix box, enter the first digit of the extension numbers range in which the MCU resides.
- f. Select the **Refresh H.323 Registrations** check box, and select **120 seconds**.
8. On the Spans tab, add a new IP Span.
- a. In the **Circuit ID** box, enter a unique identifier for this new circuit.
- b. In the **IP Address** box, enter the IP address of the IP card that will use H.323 signaling.
- c. In the **H323 Alias 1** box, enter an H.323 ID of an alias for the board that Avaya Communication Manager will route calls to this MGC.
9. Define the IP1 configuration. In the **Circuit ID** box on the IP-Network Parameters tab, enter the unique identifier you specified in Step 6.
10. Create a meeting room in **Meeting Rooms and Entry Queues**. In the **Numeric ID** box on the General tab, enter the dialed digits excluding the prefix defined in the Network Service.

If you want to configure Ad-hoc conferencing for the MGC system, go to [Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform](#) on page 89.

Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server

This section provides a set of guidelines to configure Polycom MGC video conferencing bridge platforms for use with Avaya S8500 servers and Avaya S87xx servers. You must understand these guidelines before you administer these systems.

If you want to configure Ad-hoc conferencing for the MGC system (after you administer the MGC system for use with the Avaya server), go to [Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform](#) on page 89.

Trunk Groups

For incoming trunk groups, you must:

- Create one incoming trunk group per Polycom MGC system.
- Set the following parameters:
 - **Direction** to **incoming**.
 - **Service Type** to **tie**.
 - **Disconnect Supervision - In?** to **y** to allow Polycom MGC-Avaya Communication Manager-Polycom MGC calls (that is, trunks calling trunks).

For outgoing trunk groups, you must:

- Create one “primary” outgoing trunk group for the “primary” Polycom MGC board (IP1).
- Set the following parameters:
 - **Direction** to **outgoing**.
 - **Service Type** to **tie**.
 - You may set **Outgoing Display** to **y**.
 - **Send Calling Number** to **y**. This allows participant matching in the Polycom MGC.
 - **Format** to **private**.
- If you want board redundancy, create one “secondary” outgoing trunk group for the other boards (IP2.n) in the Polycom MGC system.

Signaling Groups

For incoming signaling groups, you must:

- Create one incoming signaling group (RRQ signaling group) per MGC board in the Polycom MGC system for a primary CLAN. This incoming signaling group allows a Polycom MGC board to register and is used for incoming calls. The “primary” CLAN is the CLAN you want to use with the MGC. The IP address of this CLAN is administered on the MGC via the Polycom MGC Manager software.

Keep in mind the following information:

- For Avaya Communication Manager Release 3.0.1, one signaling group can support a maximum of 31 calls.
- For Avaya Communication Manager Release 3.1 or later, one signaling group can support a maximum of 255 calls.
- Set the following parameters for the incoming signaling groups:
 - **IP Video?** to **y**.
 - **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
 - **Trunk Group for Channel Selection**.
 - **Near-end Listen Port** to **1720**.
 - **Far-end Listen Port** to **1720**.
 - **ARQ Required?** to **y**.
 - **RRQ Required?** to **y**.
 - **Enable Layer 3 Test** to **n**.
 - **Direct IP-IP Audio Connections to?** to **y**.
 - **Far-end Network Region**. If you set the maximum bandwidth for video calls in an IP network region, assign the appropriate IP network region.
- Optional: Create one incoming signaling group per MGC board in the Polycom MGC system for a secondary CLAN. If the primary CLAN fails, the MGC will use the alternate gatekeeper list as a list of alternate CLANs with which to register.

Setting Up Video Endpoints

For outgoing signaling groups, you must:

- Create one outgoing signaling group (LRQ signaling group) per board in the Polycom MGC system for the primary CLAN. This outgoing signaling group is used for outgoing LRQ calls to the co-resident gatekeeper in the Polycom MGC system.

Keep in mind the following information:

- For Avaya Communication Manager Release 3.0.1, one signaling group can support a maximum of 31 calls.
- For Avaya Communication Manager Release 3.1 or later, one signaling group can support a maximum of 255 calls.
- Set the following parameters for the outgoing signaling groups:
 - **IP Video?** to **y**.
 - **Near-end Listen Port** to **1719**.
 - **Far-end Listen Port** to **1719**.
 - **LRQ Required?** to **y**.
 - **Enable Layer 3 Test** to **n**.
 - **Direct IP-IP Audio Connections to?** to **y**.
 - **Far-end Network Region**. If you set the maximum bandwidth for video calls in an IP network region, assign the appropriate IP network region.

Note:

Do not set Trunk Group for Channel Selection. If you set this parameter, all incoming video calls may fail or video may close during audio shuffle.

- Optional: Create one outgoing signaling group per board in the Polycom MGC system for the secondary CLAN.
- Optional: Create additional outgoing signaling groups per board in the Polycom MGC system per CLAN for additional CLAN load sharing and additional call capacity.

Group Member Assignments

Keep in mind the following information:

- Group member assignments for the incoming trunk may consist of all incoming signaling groups for the Polycom MGC system.
- Group member assignments for the primary outgoing trunk may consist of all signaling groups defined for multiple CLANs to the one primary board in the Polycom MGC system.
Do not mix Polycom MGC boards.
- Group member assignments for the secondary outgoing trunk may consist of all signaling groups defined for multiple CLANs to the other boards in the Polycom MGC system.

Outgoing Rules

Keep in mind the following information:

- Change dial plan analysis and uniform dial plan as required to support the Polycom MGC-assigned extension range.
- Add AAR analysis for dial plan extension range for use by the Polycom MGC system. Use **lev0** as the type to force use of the private numbering plan.
- On the route pattern form, add an entry for each outgoing trunk group, and set **LAR** to next. Only one route pattern should be required per Polycom MGC system.
- Regarding digit manipulation, present the digits to the Polycom MGC system in the form of “prefix” plus digits. For example, suppose the Polycom MGC system is administered with the prefix **7**, and there is a five-digit dial plan with **715xx** routing to the Polycom MGC system. You should present the digits **715xx** instead of **15xx**, where **15xx** is the meeting rooms. The Polycom MGC system allows support of multiple prefixes.

Examples

Example 1: S87xx with 2 CLANs/MGC-50 with 2 boards, board redundancy, and no CLAN redundancy

In this example, CLAN1 is chosen as the CLAN for use with the Polycom MGC system. CLAN2 is not used. If CLAN1 fails, the Polycom MGC system will not be allowed to register to CLAN2 and will no longer be able to make incoming or outgoing calls. If the Polycom MGC board IP1 fails, IP2 will continue to be able to make incoming and outgoing calls.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members

SigGroup 2: CLAN1, IP2; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 3: CLAN1, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 4: CLAN1, IP2; 31 trunk members

Example 2: S87xx with 2 CLANs/MGC-50 with 2 boards, board redundancy, and CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members

SigGroup 2: CLAN1, IP2; 31 trunk members

SigGroup 3: CLAN2, IP1; 31 trunk members

SigGroup 4: CLAN2, IP2; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 5: CLAN1, IP1; 31 trunk members

SigGroup 6: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 7: CLAN1, IP2; 31 trunk members

SigGroup 8: CLAN2, IP2; 31 trunk members

Example 3: S87xx with 2 CLANs/MGC-50 with 3 boards, board redundancy, and CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 and IP3 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members
SigGroup 3: CLAN1, IP3; 31 trunk members
SigGroup 4: CLAN2, IP1; 31 trunk members
SigGroup 5: CLAN2, IP2; 31 trunk members
SigGroup 6: CLAN2, IP3; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 7: CLAN1, IP1; 31 trunk members
SigGroup 8: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 9: CLAN1, IP2; 31 trunk members
SigGroup 10: CLAN2, IP2; 31 trunk members
SigGroup 11: CLAN1, IP3; 31 trunk members
SigGroup 12: CLAN2, IP3; 31 trunk members

Example 4: S87xx with 4 CLANs/MGC-50 with 3 boards, board redundancy, and outgoing CLAN redundancy

In this example, CLAN1 is chosen as the primary CLAN for the Polycom MGC system to use, and CLAN2 is a backup. CLAN2 provides backup to CLAN1 for Polycom MGC registration and incoming and outgoing calls. If Polycom MGC board IP1 fails, IP2 and IP3 will continue to be able to make incoming and outgoing calls.

Note that the incoming signaling groups for CLAN2 will be out-of-service unless the Polycom MGC boards are forced to register with CLAN2 in the event that CLAN1 is unavailable.

Note that CLAN3 and CLAN4 are not used. Additional outgoing call capacity could be added by defining additional outgoing signaling groups between CLAN3 to IP1, IP2, and IP3, and CLAN4 to IP1, IP2, and IP3. Additional incoming call capacity could be added by defining additional incoming signaling groups between CLAN3 and CLAN4 to boards IP1, IP2, and IP3.

Trunk 1: MGC-A Incoming:

SigGroup 1: CLAN1, IP1; 31 trunk members
SigGroup 2: CLAN1, IP2; 31 trunk members
SigGroup 3: CLAN1, IP3; 31 trunk members
SigGroup 4: CLAN2, IP1; 31 trunk members
SigGroup 5: CLAN2, IP2; 31 trunk members
SigGroup 6: CLAN2, IP3; 31 trunk members

Trunk 2: MGC-A Outgoing Primary:

SigGroup 7: CLAN1, IP1; 31 trunk members
SigGroup 8: CLAN2, IP1; 31 trunk members

Trunk 3: MGC-A Outgoing Secondary:

SigGroup 9: CLAN1, IP2; 31 trunk members
SigGroup 10: CLAN2, IP2; 31 trunk members
SigGroup 11: CLAN1, IP3; 31 trunk members
SigGroup 12: CLAN2, IP3; 31 trunk members

Configure Ad-hoc Video Conferencing for a Polycom MGC Video Conferencing Bridge Platform

This section describes how to configure Ad-hoc video conferencing for a Polycom MGC video conferencing bridge platform.

Checklist

When setting up Ad-hoc video conferencing for a Polycom MGC, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the MGC system
- the IP address of the CLAN

Configuration Procedures

To configure Ad-hoc conferencing, you must perform the following steps:

1. Configure the IP network regions for the MGC.
2. Configure the MGC for use with an Avaya server.
3. Determine the maximum number of Ad-hoc video conferencing ports your voice system supports.
4. Configure the Class of Service for Ad-hoc video conferencing.
5. Configure a video bridge.
6. Configure the MGC system.

Note:

Keep in mind the following information when configuring the Polycom MGC:

- Place the Polycom MGC in a dedicated network region with a dedicated codec set to infer the conference bit rates.
- Ensure that you specify the correct network region (Far-end Network Region field) when you add the signaling groups for the MGC (Signaling Group form).
- Ensure that all other network regions have direct connectivity to the MGC's network region (**change ip-network-region** command).

Procedure 1: Configure IP Network Regions

You must place the Polycom MGC in a dedicated network region and ensure that all other network regions have direct connectivity to the Polycom MGC's network region.

To configure the IP network regions:

1. Use the **change ip-network-region x** command (where **x** is the chosen IP network region) to access the IP Network Region form for the specified region.

The IP Network Region form appears.

Figure 18: Example of Page 1 of the IP Network Region Form

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
IP NETWORK REGION																		
Region: 3																		
Location: <input type="text"/>			Authoritative Domain: <input type="text"/>															
Name: <input type="text"/>																		
MEDIA PARAMETERS																		
Codec Set: <input type="text" value="3"/>			Intra-region IP-IP Direct Audio: <input type="text" value="yes"/>															
UDP Port Min: <input type="text" value="2048"/>			Inter-region IP-IP Direct Audio: <input type="text" value="yes"/>															
UDP Port Max: <input type="text" value="3329"/>			IP Audio Hairpinning? <input type="text" value="y"/>															
DIFFSERV/TOS PARAMETERS																		
Call Control PHB Value: <input type="text" value="46"/>			RTCP Reporting Enabled? <input type="text" value="y"/>															
Audio PHB Value: <input type="text" value="46"/>			RTCP MONITOR SERVER PARAMETERS															
Video PHB Value: <input type="text" value="26"/>			Use Default Server Parameters? <input type="text" value="y"/>															
802.1P/Q PARAMETERS																		
Call Control 802.1p Priority: <input type="text" value="6"/>																		
Audio 802.1p Priority: <input type="text" value="6"/>																		
Video 802.1p Priority: <input type="text" value="5"/>			AUDIO RESOURCE RESERVATION PARAMETERS															
H.323 IP ENDPOINTS																		
H.323 Link Bounce Recovery? <input type="text" value="y"/>			RSVP Enabled? <input type="text" value="n"/>															
Idle Traffic Interval (sec): <input type="text" value="20"/>																		
Keep-Alive Interval (sec): <input type="text" value="5"/>																		
Keep-Alive Count: <input type="text" value="5"/>																		

2. Set **Intra-region IP-IP Direct Audio** to **yes**.
3. Set **Inter-region IP-IP Direct Audio** to **yes**.

Note:

Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

4. Go to page 2 of the form.

Figure 19: Example of Page 2 of the IP Network Region Form

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----

IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY

Incoming LDN Extension:

Conversion To Full Public Number - Delete: ☐ Insert:

Maximum Number of Trunks to Use for IGAR:

Dial Plan Transparency in Survivable Mode? ☒ n

BACKUP SERVERS(IN PRIORITY ORDER)	H.323 SECURITY PROFILES
1 <input type="text"/>	1 <input type="text" value="any-auth"/>
2 <input type="text"/>	2 <input type="text"/>
3 <input type="text"/>	3 <input type="text"/>
4 <input type="text"/>	4 <input type="text"/>
5 <input type="text"/>	
6 <input type="text"/>	

Allow SIP URI Conversion? ☒ y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS

Near End Establishes TCP Signaling Socket? ☒ y

Near End TCP Port Min:

Near End TCP Port Max:

5. Set **Security Procedures 1** to **any-auth**.
6. Go to page 3 of the form.
7. Set **codec set** to the appropriate codec set you defined.
8. Set **Video Norm** to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region.
9. Set **Video Prio** to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region.
10. Set **Video Shr**. Specify whether the normal video pool can be shared with the audio pool for each link between IP network regions (**y** or **n**).
11. Repeat Steps 1 through 10 for each IP network region that will be used for video in this system.

Procedure 2: Configure the Polycom RMX for Use with an Avaya Server

Perform the procedures in the appropriate section to configure the Polycom MGC system:

1. [Configure a Polycom MGC-25 Video Conferencing Bridge Platform for an Avaya S8300 Server](#) on page 78.
2. [Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server](#) on page 82.

After performing these procedures, go to [Procedure 3: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported](#) on page 92.

Procedure 3: Determine the Maximum Number of Ad-hoc Video Conferencing Ports Supported

To determine the maximum number of Ad-hoc video conferencing ports your voice system supports:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48. This is a license count that Avaya provides based on your stated needs. Licensing and administration are two different decisions on port counts.

Figure 20: Example of Page 2 of the Optional Features Form

1	2	3	4	5	6	7	8	9	10
OPTIONAL FEATURES									
IP PORT CAPACITIES									
Maximum Administered H.323 Trunks: 200									USED 174
Maximum Concurrently Registered IP Stations: 40									7
Maximum Administered Remote Office Trunks: 0									0
Maximum Concurrently Registered Remote Office Stations: 0									0
Maximum Concurrently Registered IP eCons: 10									0
Max Concur Registered Unauthenticated H.323 Stations: 10									0
Maximum Video Capable Stations: 40									20
Maximum Video Capable IP Softphones: 40									14
Maximum Administered SIP Trunks: 100									70
Maximum Administered Ad-hoc Video Conferencing Ports: 217									100
Maximum Number of DS1 Boards with Echo Cancellation: 0									0
Maximum TN2501 VAL Boards: 0									0
Maximum Media Gateway VAL Sources: 0									0
Maximum TN2602 Boards with 80 VoIP Channels: 0									0
Maximum TN2602 Boards with 320 VoIP Channels: 0									0
Maximum Number of Expanded Meet-me Conference Ports: 0									0
(NOTE: You must logoff & login to effect the permission changes.)									

In this example, the system can have a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

Procedure 4: Configure Class of Service

To configure the Class of Service for Ad-hoc video conferencing:

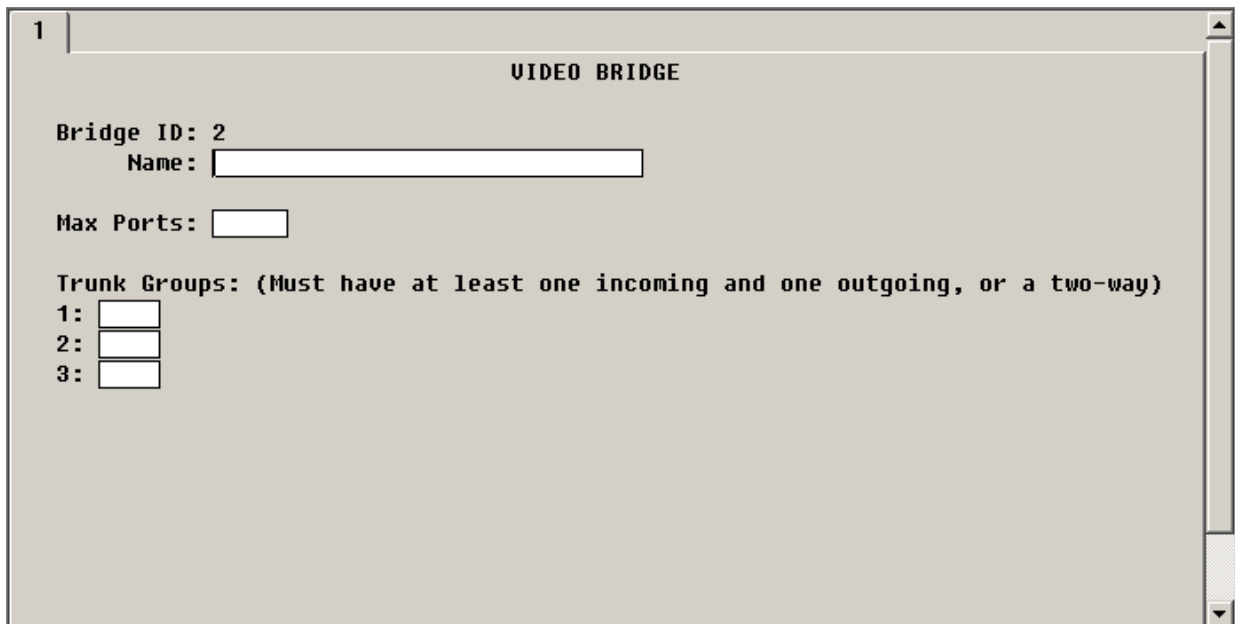
1. Use the **change cos** command to access the Class of Service form.
2. Go to page 2 of the form.
3. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.

Procedure 5: Configure a Video Bridge

To configure a video bridge:

1. Use the **add video-bridge xx** command (where **xx** is the bridge number between 1 to 40, and each video bridge belongs to an MCU) to access the Video Bridge form.

Figure 21: Example of the Video Bridge Form



The screenshot shows a web-based configuration form titled "VIDEO BRIDGE". The form is displayed in a browser window with a tab labeled "1". The form contains the following fields and labels:

- Bridge ID:** 2
- Name:** [Text input field]
- Max Ports:** [Text input field]
- Trunk Groups:** (Must have at least one incoming and one outgoing, or a two-way)
- 1:** [Text input field]
- 2:** [Text input field]
- 3:** [Text input field]

2. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - MGC25*).
3. Set **Max Ports** to the maximum number of Ad-hoc conferencing ports you want to assign to this bridge. (The minimum you can enter is 3.) This is equivalent to the number of ports that are available for Ad-hoc use on the associated MGC based on a needed bit rate for video.
4. In **Trunk Groups**, enter the administered incoming or outgoing ISDN H.323 or SIP trunk groups you added for the MGC. All entries must be of the same carrier type (that is, all H.323 trunks or all SIP trunks).

The Far End Resource Info, ID Range, Priority Factory Number, and Standard Factory Number fields appear.

Note:

MGC Ad-hoc should not be used for SIP video endpoints. Expect no video.

5. Set **Far End Resource Info?** to **n**. The Priority Factory Number and Standard Factory Number fields are removed.

6. Set **ID Range** to the range of ports. These IDs correspond to the actual conference ID numbers of meeting rooms configured on the MGC. For example, if you enter the range 1000 - 1003, you must configure 1000, 1001, 1002, and 1003 as meeting rooms on the MGC. These meeting rooms are for Ad-hoc use only and must not be accessible via the Unified Dial Plan (UDP). Note that Automatic Alternate Routing (AAR) and Unified Dial Plan are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan. As a result, you can set up several video bridges with exactly the same conference IDs and numbers. (This will make it easier for you to maintain configurations and swap hardware.)

Procedure 6: Configure the MGC System

On the MGC system, perform the following steps for Ad-hoc conferencing:

1. Create meeting room IDs that correspond to the ID range on Avaya Communication Manager Video Bridge form, with each being video switching auto conferences. Determine the ID length from the MGC system.cfg file.
2. Set 1*1 transcoding so cascaded conferences display properly.

Display Capacity for Ad-hoc Video Conferencing

To display the capacity for Ad-hoc video conferencing:

1. Use the **display capacity** command to access the System Capacity form.
2. Go to page 7. Ad-hoc Video Conferencing Ports displays the following Ad-hoc video conferencing information:
 - Used - the number of video conferencing ports currently in use.
 - Available - the number of video conferencing ports currently available.
 - System Limit - the total number of video conference ports in your system. (This is the sum of Used ports and Available ports.)

View Video Conferencing Bridges

Use the **list video-bridge** command to view the video conferencing bridges administered on your system.

Configure an Avaya Meeting Exchange 5.0.1 S6800 Bridge

This section describes how to configure an Avaya Meeting Exchange 5.0.1 S6800 bridge as an external video bridge.

Checklist

When setting up an Avaya Meeting Exchange 5.0.1 S6800 bridge, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the Priority Factory Number and the Standard Factory Number to use in the Avaya Communication Manager system and the Avaya Meeting Exchange bridge.

Things to Keep in Mind

Before configuring an Avaya Meeting Exchange 5.0.1 S6800 bridge, keep in mind the following information:

- For more information on the Avaya Meeting Exchange bridge, refer to the Avaya Meeting Exchange 5.0.1 Installation and Administrator guide.
- Ad-hoc supports six audio callers per conference.
- Schedule supports 16 video callers per Meeting Exchange 5.0.1 scheduled conference.
- Each 6800 bridge can support up to 2000 video ports
- Each conference can support up to 16 video participant.
- The video capacity for each Convedia MPC varies depending on bit rate, picture size, and frame rate. See the following table.

Table 11: Video Capacity

Total Bit Rate	Picture Size (MPI)	Audio Codec	# Ports per MPC	Resource Allocation for Video (%)
768 Kbit/s	CIF:1	G.711	45	91
384 Kbit/s	CIF:2	G.711	90	75
128 Kbit/s	QCIF:4	G.711	250	75

Configuration Procedures

To configure an Avaya Meeting Exchange 5.0.1 S6800 bridge with an Avaya Communication Manager system, you must perform the following steps:

1. Verify the licensing on the Avaya Communication Manager system.
2. Configure IP network regions for the Meeting Exchange system.
3. Add an entry in the IP node names for the Meeting Exchange system.
4. Add a signaling group for the Meeting Exchange system.
5. Add a SIP trunk group for the Meeting Exchange system.
6. Configure the Avaya Meeting Exchange 5.0.1 S6800 bridge.
7. Configure the Radisys CMS 6000 for Avaya Meeting Exchange 5.0.1 S6800 bridge.
8. Configure Avaya Communication Manager Video Bridge (Ad-hoc conferencing only).
9. Configure Avaya Communication Manager to use SES for Avaya Meeting Exchange.

Procedure 1: Verify Licensing

You must verify that the Avaya Communication Manager system is licensed for video endpoints, Ad-hoc video conferencing ports, and multimedia IP SIP trunking.

To verify licensing:

1. Use the **display system-parameters customer-options** command to access the Optional Features form.
2. On page 2 of the form, verify the following settings:
 - **Maximum Video Capable IP Softphones.** This number is provided by the RFA license file.

Note:

To provide video softphone capability, you must have at least this number of IP Softphone licenses. Page 10 of this form displays the number of IP Softphone licenses you have.

- **Maximum Administered Ad-hoc Video Conferencing Ports.** The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48.

Figure 22: Example of Page 2 of the Optional Features Form

1	2	3	4	5	6	7	8	9	10
OPTIONAL FEATURES									
IP PORT CAPACITIES									USED
Maximum Administered H.323 Trunks: 200									174
Maximum Concurrently Registered IP Stations: 40									7
Maximum Administered Remote Office Trunks: 0									0
Maximum Concurrently Registered Remote Office Stations: 0									0
Maximum Concurrently Registered IP eCons: 10									0
Max Concur Registered Unauthenticated H.323 Stations: 10									0
Maximum Video Capable Stations: 40									20
Maximum Video Capable IP Softphones: 40									14
Maximum Administered SIP Trunks: 100									70
Maximum Administered Ad-hoc Video Conferencing Ports: 217									100
Maximum Number of DS1 Boards with Echo Cancellation: 0									0
Maximum TN2501 UAL Boards: 0									0
Maximum Media Gateway UAL Sources: 0									0
Maximum TN2602 Boards with 80 VoIP Channels: 0									0
Maximum TN2602 Boards with 320 VoIP Channels: 0									0
Maximum Number of Expanded Meet-me Conference Ports: 0									0
(NOTE: You must logoff & login to effect the permission changes.)									

In this example, the system can have:

- a maximum of 40 video-enabled Avaya IP Softphones. Currently, 13 video-capable Avaya IP Softphones are being used.
- a maximum of 217 administered Ad-hoc video conferencing ports. Currently, 100 Ad-hoc video conferencing ports are being used.

3. Go to page 4.

Figure 23: Example of Page 4 of the Customer-Options Form

1	2	3	4	5	6	7	8	9	10	11
OPTIONAL FEATURES										
Emergency Access to Attendant? <input checked="" type="checkbox"/>						IP Stations? <input checked="" type="checkbox"/>				
Enable 'dadmin' Login? <input checked="" type="checkbox"/>						ISDN Feature Plus? <input checked="" type="checkbox"/>				
Enhanced Conferencing? <input checked="" type="checkbox"/>						ISDN/SIP Network Call Redirection? <input checked="" type="checkbox"/>				
Enhanced EC500? <input checked="" type="checkbox"/>						ISDN-BRI Trunks? <input checked="" type="checkbox"/>				
Enterprise Survivable Server? <input checked="" type="checkbox"/>						ISDN-PRI? <input checked="" type="checkbox"/>				
Enterprise Wide Licensing? <input checked="" type="checkbox"/>						Local Survivable Processor? <input checked="" type="checkbox"/>				
ESS Administration? <input checked="" type="checkbox"/>						Malicious Call Trace? <input checked="" type="checkbox"/>				
Extended Cvg/Fwd Admin? <input checked="" type="checkbox"/>						Media Encryption Over IP? <input checked="" type="checkbox"/>				
External Device Alarm Admin? <input checked="" type="checkbox"/>						Mode Code for Centralized Voice Mail? <input checked="" type="checkbox"/>				
Five Port Networks Max Per MCC? <input checked="" type="checkbox"/>						Multifrequency Signaling? <input checked="" type="checkbox"/>				
Flexible Billing? <input checked="" type="checkbox"/>						Multimedia Call Handling (Basic)? <input checked="" type="checkbox"/>				
Forced Entry of Account Codes? <input checked="" type="checkbox"/>						Multimedia Call Handling (Enhanced)? <input checked="" type="checkbox"/>				
Global Call Classification? <input checked="" type="checkbox"/>						Multimedia IP SIP Trunking? <input checked="" type="checkbox"/>				
Hospitality (Basic)? <input checked="" type="checkbox"/>										
Hospitality (G3V3 Enhancements)? <input checked="" type="checkbox"/>										
IP Trunks? <input checked="" type="checkbox"/>										
IP Attendant Consoles? <input checked="" type="checkbox"/>										
(NOTE: You must logoff & login to effect the permission changes.)										

4. Make sure **Multimedia IP SIP Trunking?** is set to **y**.

Procedure 2: Configure IP Network Regions

You must place the Meeting Exchange system in a dedicated network region and ensure that all other network regions have direct connectivity to the Meeting Exchange system's network region.

To configure the IP network regions:

1. Use the **change ip-network-region x** command (where **x** is the chosen IP network region) to access the IP Network Region form for the specified region.

The IP Network Region form appears.

Figure 24: Example of Page 1 of the IP Network Region Form

```

change ip-network-region 11
Page 1 of 19

IP NETWORK REGION

Region: 11
Location:   Authoritative Domain: du.rnd.avaya.com
Name: MX

MEDIA PARAMETERS
Codec Set: 1 Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? n
UDP Port Max: 3329

DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46 RTCP Reporting Enabled? y
Audio PHB Value: 46 RTCP MONITOR SERVER PARAMETERS
Video PHB Value: 26 Use Default Server Parameters? y

802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
  
```

2. Set **Authoritative Domain** for IP network regions that contain SIP endpoints/MCUs.
3. Set **Intra-region IP-IP Direct Audio** to **yes**.
4. Set **Inter-region IP-IP Direct Audio** to **yes**.

Note:

Shuffling is recommended. However, you can set shuffling to **no**, and video calls will work properly.

5. Go to page 2 of the form.

Figure 25: Example of Page 2 of the IP Network Region Form

```
change ip-network-region 11                                     Page 2 of 19
IP NETWORK REGION

INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY
Incoming LDN Extension: 
Conversion To Full Public Number - Delete: _ Insert: 
Maximum Number of Trunks to Use for IGAR: 
Dial Plan Transparency in Survivable Mode? n

BACKUP SERVERS (IN PRIORITY ORDER)      H.323 SECURITY PROFILES
1                                     1 any-auth
2                                     2 
3                                     3 
4                                     4 
5                                     5 
6                                     6 
Allow SIP URI Conversion? y

TCP SIGNALING LINK ESTABLISHMENT FOR AVAYA H.323 ENDPOINTS
Near End Establishes TCP Signaling Socket? y
Near End TCP Port Min: 61440
Near End TCP Port Max: 61444
```

6. Set **H.323 SECURITY PROFILES 1** to **any-auth**.
7. Go to page 3 of the form.

Figure 26: Example of Page 3 of the IP Network Region Form

135.64.24.40 - PuTTY

change ip-network-region 11 Page 3 of 19

Inter Network Region Connection Management

src rgn	dst rgn	codec set	direct WAN	Units	WAN-BW-limits	Video	Dyn
11	1	1	y	NoLimit			n
11	2						
11	3	1	y	NoLimit			n
11	4	1	y	NoLimit			n
11	5	1	y	NoLimit			n
11	6						
11	7						
11	8						
11	9						
11	10						
11	11	1					
11	12						
11	13						
11	14						
11	15						

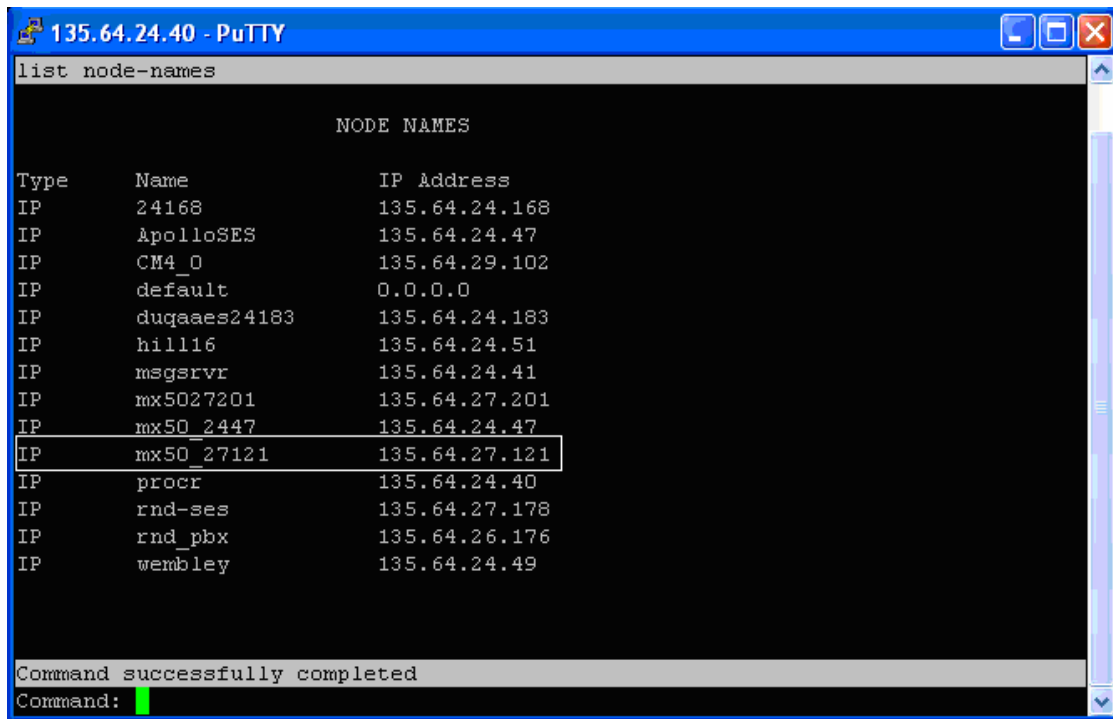
8. Set **codec set** to the appropriate codec set you defined.
9. Set **Units** to **NoLimit** for each destination IP network region. You can set unlimited bandwidth or use the bandwidth management option by restricting the bandwidth.
10. Repeat Steps 1 through 9 for each IP network region that will be used for video in this system.

Procedure 3: Add an Entry in the IP Node Names for the Meeting Exchange System

To add an entry in the IP Node Names form for the Meeting Exchange system:

1. Use the **change node-names ip** command to access the IP Node Names form.

Figure 27: Example of Page 1 of the IP Node Names Form



```
list node-names
```

Type	Name	IP Address
IP	24168	135.64.24.168
IP	ApolloSES	135.64.24.47
IP	CM4_0	135.64.29.102
IP	default	0.0.0.0
IP	duqaes24183	135.64.24.183
IP	hill16	135.64.24.51
IP	msgsrvr	135.64.24.41
IP	mx5027201	135.64.27.201
IP	mx50_2447	135.64.24.47
IP	mx50_27121	135.64.27.121
IP	procr	135.64.24.40
IP	rnd-ses	135.64.27.178
IP	rnd_pbx	135.64.26.176
IP	wembley	135.64.24.49

Command successfully completed

Command:

2. In the **Name** field, enter a name for the Meeting Exchange S6200 system.
3. In the corresponding **IP Address** field, enter the IP address of the Meeting Exchange Application server.

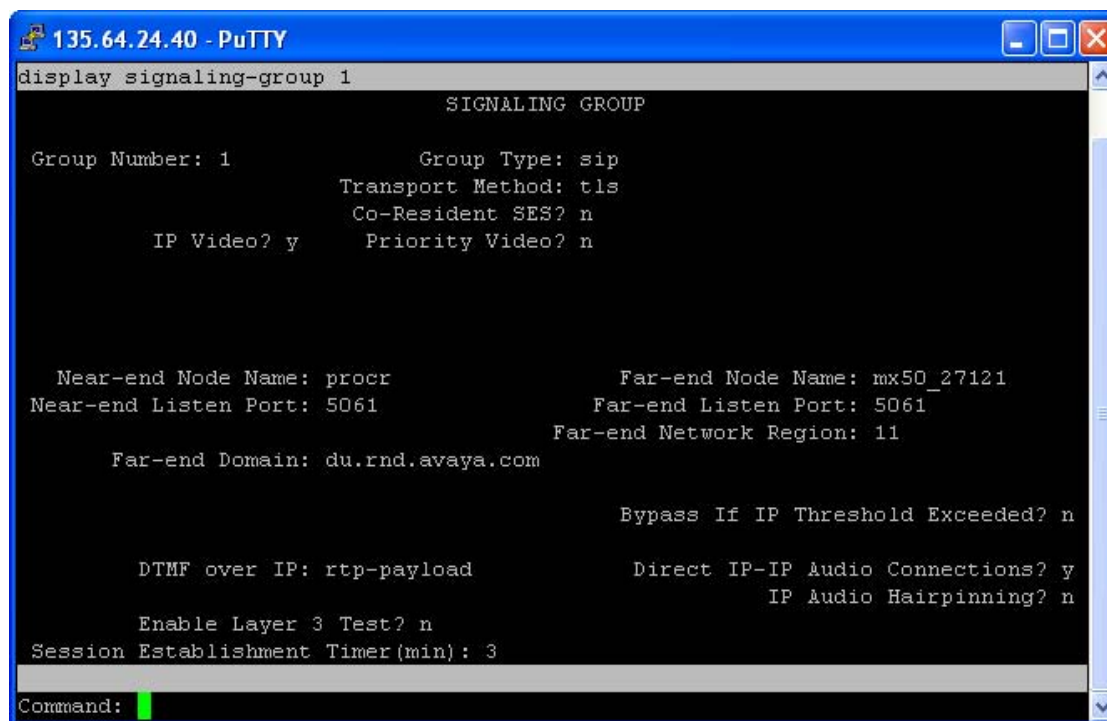
Procedure 4: Add a Signaling Group for the Meeting Exchange System

To add a signaling group for the Meeting Exchange system:

1. Use the **add signaling-group xx** command (where **xx** is the chosen signaling group) to access the Signaling Group form.

The Signaling Group form appears.

Figure 28: Example of Page 1 of the Signaling Group Form



```
135.64.24.40 - PuTTY
display signaling-group 1

SIGNALING GROUP

Group Number: 1          Group Type: sip
                        Transport Method: tls
                        Co-Resident SES? n
                        IP Video? y      Priority Video? n

Near-end Node Name: procr      Far-end Node Name: mx50_27121
Near-end Listen Port: 5061     Far-end Listen Port: 5061
Far-end Network Region: 11
Far-end Domain: du.rnd.avaya.com

Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload      Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n

Enable Layer 3 Test? n
Session Establishment Timer(min): 3

Command: 
```

2. Set **Group Type** to **sip**.
3. Set **Transport Method** to **tls** or **tcp**.
4. Set **IP Video** to **y**.
5. Set **Priority Video** as appropriate.
6. Set **Near-end Node Name**. For example, for an S8300 system, you would enter **procr**. For an S8500 or S8700 system, you would enter the name of the CLAN board.
7. Set **Near-end Listen Port** to **5061** or **5060**.
8. Set **Far-end Node Name** to the name you entered for the Meeting Exchange system.
9. Set **Far-end Listen Port** to **5061** or **5060**.
10. Set **Far-end Network Region** to the network region you specified for the Meeting Exchange system.
11. Set **Session Establishment Timer (min)** to **120**.
12. Set **DTMP over IP** to **in-band**.
13. Set **Enable Layer 3 Test** to **n**.
14. Set **Direct IP-IP Audio Connected** to **y**.

Procedure 5: Add a SIP Trunk Group for the Meeting Exchange System

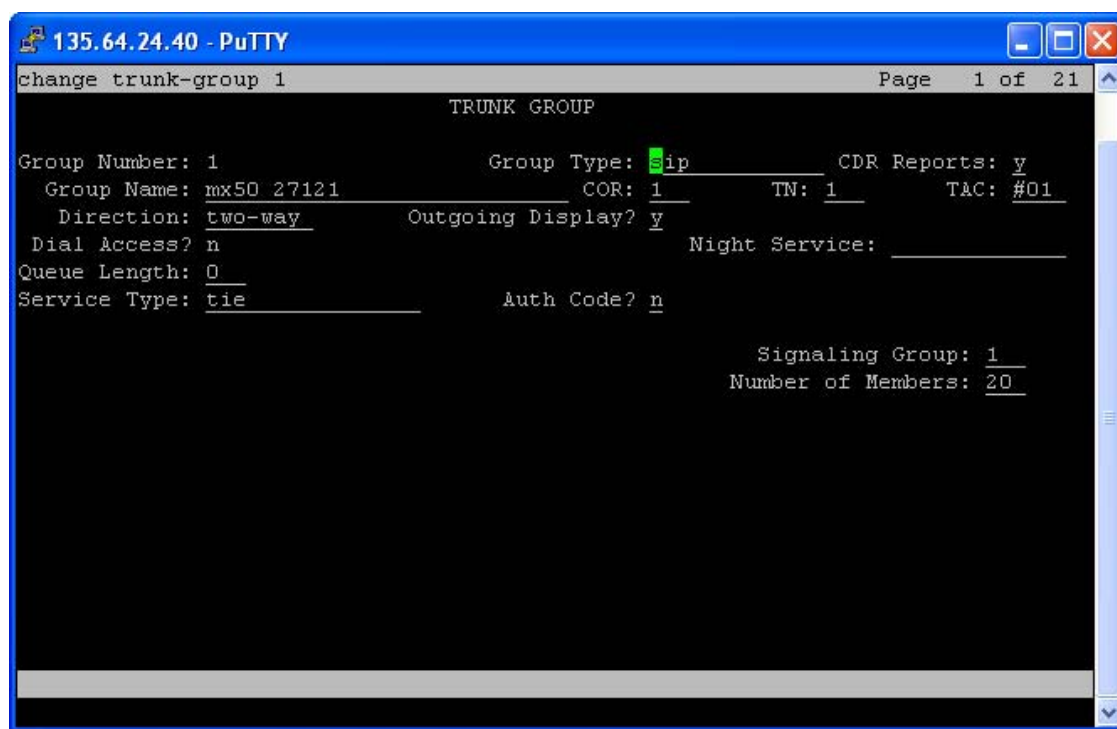
You must administer a SIP trunk group for the Meeting Exchange system.

Perform the following steps:

1. Use the **add trunk-group xx** command (where **xx** is the chosen trunk group) to access the Trunk Group form.

The Trunk Group form appears.

Figure 29: Example of Page 1 of the Trunk Group Form



```

135.64.24.40 - PuTTY
change trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                      Group Type: sip      CDR Reports: y
Group Name: mx50 27121                COR: 1             TN: 1       TAC: #01
Direction: two-way                    Outgoing Display? y
Dial Access? n                        Night Service:
Queue Length: 0
Service Type: tie                     Auth Code? n
                                     Signaling Group: 1
                                     Number of Members: 20
  
```

- a. Set **Group Type** to **sip**.
- b. Set **Group Name** to the name of the Meeting Exchange system (for example, Avaya Meeting Exchange 5.0.1 SIP Bridge).
- c. Set **COR**.
- d. Set **Direction** to **two-way**.
- e. Set **Outgoing Display** to **y** to display caller ID (from the Station form).
- f. Set **Service Type** to **tie**.
- g. Set **Signaling Group** to the signaling group you created for the Meeting Exchange system.
- h. Set **Number of Members**.

Procedure 6: Configure the Avaya Meeting Exchange 5.0.1 S6800 Bridge

In this section, you will:

1. Configure the Meeting Exchange bridge for TLS or TCP so it will be able to communicate with Avaya Communication Manager.
2. Configure the non-Ad-hoc video conferencing parameters for the Meeting Exchange bridge.
3. Configure the call branding digits that you will use to dial into the Meeting Exchange bridge.
4. Configure the dial outs for the Meeting Exchange bridge.
5. Configure Avaya Meeting Exchange 5.0.1 for Radisys CMS 6000.
6. Configure the Ad-hoc video conferencing parameters on the Meeting Exchange bridge.
7. Schedule conferences on Avaya Meeting Exchange 5.0.1 to ensure correct operation.

Note:

You must log into the Meeting Exchange bridge using ssh with craft and su to sroot. All configuration changes except cbutil require a system reboot for the changes to take effect.

To configure the Meeting Exchange bridge:

1. Using a text editor, open the file /usr/ipcb/config/system.cfg, and make sure the following parameters are configured:
 - MyListener
 - respContact
 - MaxChannelCount
 - MaxVideoChannelsAllowed

The following is an example of a TLS configuration:

```
# ip address of the server
IPAddress=xxx.xxx.xxx.xxx
#request we will be listening to
#TLS
MyListener=sip:6000@xxx.xxx.xxx.xxx:5061;transport=tls
#TLS
respContact=<sip:6000@xxx.xxx.xxx.xxx:5061;transport=tls>
#Audio port licensing depends on customer
MaxChannelCount=750
# video port licensing depends on customer
MaxVideoChannelsAllowed=125
```

Setting Up Video Endpoints

The following is an example of a TCP configuration:

```
# ip address of the server
IPAddress=xxx.xxx.xxx.xxx
#request we will be listening to
MyListener=sip:6000@xxx.xxx.xxx.xxx:5060;transport=tcp
#if this setting is populated will Overwrite the contact field in responses
respContact=<sip:6000@xxx.xxx.xxx.xxx:5060;transport=tcp>
#Audio port licensing depends on customer
MaxChannelCount=750
# video port licensing depends on customer
MaxVideoChannelsAllowed=125
```

2. Using a text editor, open the file `/usr/ipcb/config/mediaServerInterface.cfg`, and make sure the following parameters are configured:

- **EnableVideoSupport**

Valid entries are 0 (off) and 1 (on). The default is 0.

- **VideoSI**

This parameter sets the switching interval. Valid entries are 1 through 10 seconds. The default is 2.

- **VideoSpeakersees**

Valid entries are current and previous. The default is previous.

- **VideoSize**

Valid entries are CIF and QCIF. The default is CIF.

- **VideoBandwidth**

Valid entries are 128, 192, 256, 384, 512, and 768 Kbit/s. The default is 384 Kbits/s.

- **VideoMPI**

This parameter sets the minimum picture interval. Valid entries are 1 through 32. The default is 4. (VideoMPI=1 equals 30 fps.)

The following is an example of the mediaServerInterface.cfg settings:

```
#Audio recording server
NFSServerIPAddress=xxx.xxx.xxx.xxx
MediaServerIP_1=xxx.xxx.xxx.xxx
MediaServerName_1=mpc2
MediaServerInterfaceSipListenPort_1=5050
# Video Params
# Set EnableVideoSupport to '1' to enable video support and '0' to disable
EnableVideoSupport=1
VideoSI=2
VideoSpeakersees=previous
VideoSize=QCIF or CIF
VideoBandwidth=128
VideoMPI=4
```

3. At the command prompt, type **cbutil add** to add the call branding digits that you use to dial into the bridge. You can configure:

- SCAN to prompt the user for conference codes.
- DIRECT to go directly into a pre-configured conference.

Example:

```
cbutil add 24049 0 301 1 n DIRECT -1 Adhoc in Avaya
```

DNIS	Grp	Msg	PS	CP	Function	Line Name	Company Name
-----	-----	-----	----	-----	-----	-----	-----
24047	0	247	1	N	SCAN	Schedule	Avaya
24049	0	301	1	N	DIRECT	Adhoc	Avaya

4. Using a text editor, open the file /usr/ipcb/config/telnumToURI.cfg to configure the dial outs for the Meeting Exchange bridge. Your dial outs are configured on the bridge in /usr/ipcb/config/telnumToURI.cfg. See the following example:

TelnumPattern	TelnumConversion	comment
*	"<sip:\$1@<proxyipaddress>:5061;transport=tls>"	SES Proxy
40???	"<sip:\$1<clan_address>:5061;transport=tls>"	ACM

5. Using a text editor, open the file /usr/ipcb/config/processTable.cfg to configure Avaya Meeting Exchange 5.0.1 for Radisys CMS600. The convMS process implements the Radisys CMS600 media server interface. See the following figure for an example of the processTable.cfg file.

Figure 30: Example of processTable.cfg File

```

sroot@duqaMX50L-27121:/usr/ipcb/config
# processes file, enumerates the number of processes in the network.
# will have the name of the process   Key ID and the IP address

processName      ipcKeyNumber   ProcessExe      ProcessArgs      ipAddress
route            110                noexecute
initipcb         110                noexecute       135.64.27.121
bridget700       100                noexecute       135.64.27.121
                 dspEvents/msDispatcher,netEvents/sipAgent
commsProcess     111                /usr/dcb/bin/serverComms 135.64.27.121
sipAgent         101                /usr/dcb/bin/sipagent    135.64.27.121
                 dspEvents/msDispatcher,appEvents/bridget700
msDispatcher     102                /usr/dcb/bin/msdispatcher 135.64.27.121
                 netEvents/sipAgent,appEvents/bridget700,dspEvents/mediaServer
mediaServer      103                /usr/dcb/bin/convMS      135.64.27.121
                 appEvents/msDispatcher,netEvents/msDispatcher 1
notifyService    113                noexecute        127.0.0.1:10235
snmpAgent        120                noexecute        135.64.27.121

~
~
~
"processTable.cfg" 14L, 1143C

```

6. Perform the following steps to configure the Ad-hoc video conferencing parameters on the Meeting Exchange bridge:
 - a. On Avaya Meeting Exchange 5.0.1, configure the following values in the file `usr/ipcb/config/system.cfg`:
 - AdhocConferenceURIPattern
 - AdhocMinPortsAvailable
 - AdhocDefaultConferenceSize
 - RAINotificationInterval
 - RAIHighThreshold
 - RAILowThreshold
 - MaxRAISubscribers

The following is an example of the system.cfg settings:

```
#Adhoc conference parameters
#AdhocConferenceURIPattern=<sip:AdhocDirect$1@$2>
AdhocConferenceURIPattern=<sip:A$1@$2:5061;transport=tls>
AdhocMinPortsAvailable=20
AdhocDefaultConferenceSize=6

#RAI configuration fields

# the interval in seconds at which an RAI notification is sent
# (default 60s, min 1s, max 300s)
RAINotificationInterval=60

# the upper threshold in percentage of total ports at which an
# "AlmostOutOfResources=TRUE" notification is sent
# (default 90%)
RAIHighThreshold=90

# the lower threshold in percentage of total ports at which an
# "AlmostOutOfResources=FALSE" notification is sent
# (only to clear a previous "AlmostOutOfResources=TRUE" notification)
# (default 75%)
RAILowThreshold=75

# the maximum number of RAI subscribers allowed
# (default 10 subscribers, min 0, max 10)
maxRAISubscribers=10
```

- b. On Avaya Meeting Exchange 5.0.1, configure the following values in the file `usr/ipcb/config/conferenceProfiles.cfg`. See the following figure for an example of the `conferenceProfiles.cfg` file.

Figure 31: Example of conferenceProfiles.cfg File

```

sroot@duqaMX50L-27121:/usr/fipcb/config
# Configuration file used by bridgeTranslator to map
# conference parameter profiles to a conference factory.
# The FactoryName is used to construct a conference
# factory URI of the form:
#
# FactoryName@avayaMeetingExchange.com
#
# The parameter names (with possible values in parenthesis) are:
# ModHang: Moderator Hangup (on/off)
# VMailFilter: Voice Mail Filter (on/off)
# EntryExitAnn: Entry/Exit Announcement (on/off)
#
FactoryName          ModHang          VMailFilter          EntryExitAnn
ReservationSetup     off              on                   on
ReservationSetupNoVMB on              off                  off
1005                  on              off                  off
1006                  on              off                  on
~
~
~
~
"conferenceProfiles.cfg" 18L, 733C

```

Note:

The factory settings 1005 and 1006 should be the same on the Avaya Communication Manager system (Priority Factory number=1005, Standard Factory number=1006).

- c. On Meeting Exchange 5.0.1, from sroot go to dcbmaint 116, select **System Maintenance main menu>Administration menu>Conference Scheduler**, and set:
 - **Automatic Security Codes to 7.**
 - **On-Demand Pct (%)** as per *customer* requirement. (This is a percentage of all ports used for on-demand and Ad-hoc conferences.)

See the following figure for an example of the Configure Conference Scheduler settings.

Figure 32: Example of Configure Conference Scheduler Settings

- d. On Avaya Meeting Exchange 5.0.1, configure the file `usr/ipcb/config/UriToTelnum.tab` for DNIS. This DNIS entry is used for creating an Ad-hoc conference. 24049 is DNIS for Ad-hoc. The same DNIS has to be in `cbutil` as `DIRECT`. (Refer to the `cbutil` section.) See the following figure for an example of the `UriToTelnum.tab` file.

Figure 33: Example of UriToTelnum.tab File

```

sroot@duqaMX50L-27121:/usr/ipcb/config
# Replace the 5555 prefix with the DNIS you have configured for DIRECT
# entry into adhoc conferences using cbutil.
#
#THE COMMENT COLLUM OR ANY OF THE COLLUMS SHOULD HAVE NO SPACES

TelnumPattern    TelnumConversion    comment
"*;dnis=*;*"     $2                  ddi_in_dnis_parameter_followed_by_additi
onal_parameters
"*;dnis=*"       $2                  ddi_in_dnis_parameter_not_followed_by_ad
ditional_parameters
#"*AdhocDirect*@" $2                  diamond adhoc conf supportat
"*;A*@"         24049,$2          Adhocvideo
"sip:*@"         $1                  ddiRequest Uri
"<sip:*@"        $1                  ddi Request Uri
"<sip:*"         "0000"            no Request Uri
"sip:*"          "0000"            no Request Uri
"*sip:*@"        $2                  AvayaPhoneFormat
"sips:*@"        $1                  ddiRequest Uri_secure sip
"<sips:*@"       $1                  ddi Request Uri_secure sip
"<sips:*"        "0000"            no Request Uri_secure sip
"sips:*"         "0000"            no Request Uri_secure sip
"*sips:*@"       $2                  AvayaPhoneFormat_secure sip
"                $0                  wildcard
  
```

7. Schedule conferences on Avaya Meeting Exchange 5.0.1.

Configuring Resources On-Demand

To enable FLEX conferences:

- Connect via ssh to the bridge.
- At the command prompt, type **featcfg +flex**.
- At the command prompt, type **dcbmaint 115**.
- Select **Administration Menu>Configure Scheduler**.
- Use the Page Down key to go to the second page.
- Set **On-Demand Pct (%)** (for example, 50).

Scheduling Conferences

There are two methods to schedule a conference on the bridge.

- Method 1

- a. Connect via ssh to the bridge.
- b. At the command prompt, type **dcbsched 116**.
- c. Select **Schedule Conference**.
- d. Schedule your conference.
- e. When finished, press the Esc key.

- Method 2

Install the BridgeTalk application, which is a GUI scheduler that enables you to see your active conferences easily. If you are going to use BridgeTalk, you must first configure a sign-in on the bridge.

- a. Connect via ssh to the bridge.
- b. At the command prompt, type **dcbmaint 115**.
- c. Choose **Administration Menu>Sign-In Management**, and create a sign-in.
- d. When finished, press the Esc key.
- e. Choose **View>Conference Scheduler** from the toolbar to access the Conference Scheduler. In order for you to perform any operator tasks (such as record/playback, conference listen, and accessing lines from Enter or Help Queues), you must establish an audio path.
- f. Choose **Line>Audio Path** from the BridgeTalk toolbar.
- g. Enter the number for the Operator phone to which you want to dial out. This phone must be configured on the bridge in the file `/usr/ipcb/config/telnum/ToURI.cfg` similar to the following example:

TelnumPattern	TelnumConversion	comment
40???	"< sip:\$1<clan_address>:5061;transport=tls>"	ACM

In this example, you would dial 2020 from BridgeTalk to establish this Avaya IP phone on the Operator audio path.

Procedure 7: Configure the Convedia CMS 6000 for Avaya Meeting Exchange 5.0.1 S6800

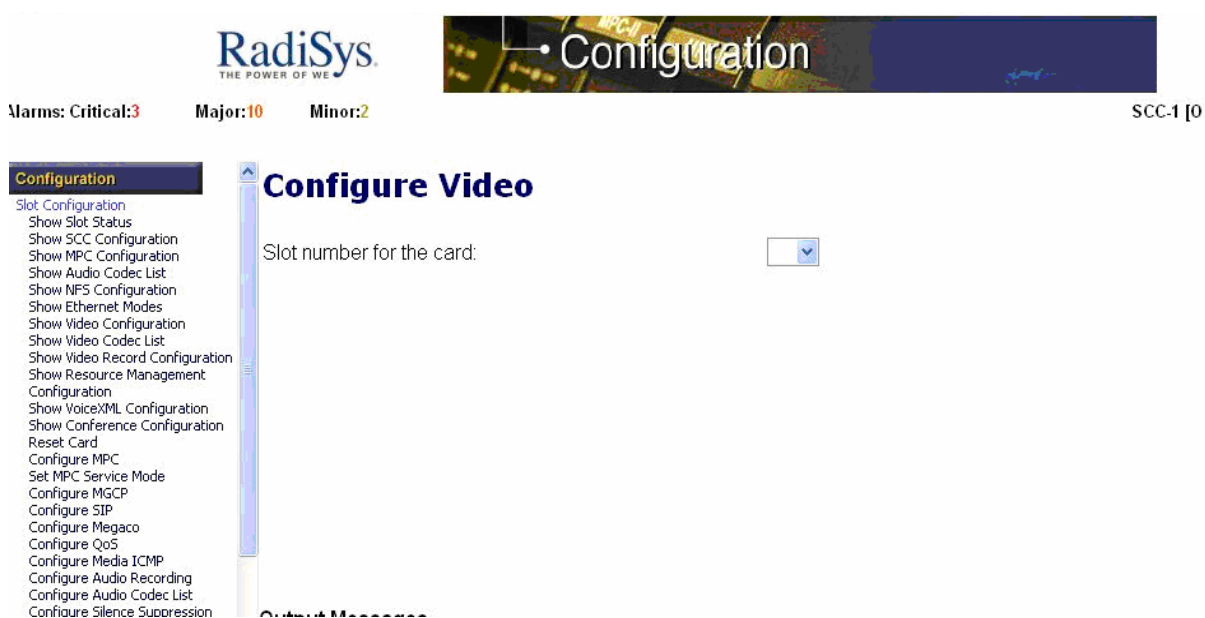
Note:

You must have administrator permission to edit the configuration and reboot the system for the changes to take effect.

To configure the Convedia CMS 6000:

1. Select **Configuration>Slot Configuration>Configure Video**.

Figure 34: Example of Configure Video Page



2. From the Slot number for the card drop-down list box, select the MPC slot.
3. Set the following parameters in the Configure Video dialog box:
 - **Video MTU to 1492.**
 - **Video Maximum Desired Bandwidth to 768.**
 - Enable the **SIP-INFO** check box in **Video I-Frame Request Method(s)**.

Figure 35: Example of Configure Video Settings

The screenshot shows the RadiSys Configuration web interface. At the top, there's a header with the RadiSys logo and a 'Configuration' banner. Below the header, there are status indicators: 'Alarms: Critical:3', 'Major:10', 'Minor:2', and 'SCC-1 [0]'. On the left, a 'Configuration' menu lists various settings like Slot Configuration, SCC Configuration, MPC Configuration, etc. The main area is titled 'Configure Video' and shows settings for 'Slot 2'. The settings include 'Video MTU' (1492), 'Video Maximum Desired Bandwidth' (768), and 'Video I-Frame Request Method(s)' with checkboxes for 'SIP-INFO' (checked) and 'RTP-FIR' (unchecked). There are 'Save Settings' and 'Reset Fields' buttons. Below the settings is an 'Output Messages' section with a scrollable text area.

4. In the Configure Video Codec List dialog box, set the following parameters for Entry #1:
 - **Codec** to **H.263**.
 - **Picture Size** to **CIF**.
 - **MPI** to **1**.

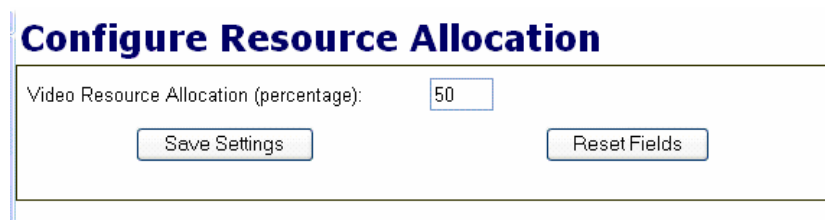
Figure 36: Example of Configure Video Codec List Settings

The screenshot shows the 'Configure Video Codec List' dialog box. It has a table with columns for 'Entry #1:', 'Codec', 'Picture Size', and 'MPI'. The values are set to 'H.263', 'CIF', and '1' respectively. There are 'Save Settings' and 'Reset Fields' buttons at the bottom.

	Codec	Picture Size	MPI
Entry #1:	H.263	CIF	1

5. In the Configure Resource Allocation dialog box, set **Video Resource Allocation (percentage)** to **50**. When resources are set to 50 percent, and the MPC contains 50 ports, 25 ports are set for video, and 25 ports are set for audio.

Figure 37: Example of Configure Resource Allocation Settings



Configure Resource Allocation

Video Resource Allocation (percentage):

Example:

1 MPC = 750 callers

50% video on MPC = 125 (Maximum video allowed per MPC = 250 > 128 bit rate)

Total audio callers can use: 375 - 125 = 250

Procedure 8: Configure Ad-hoc Conferencing on Avaya Communication Manager

To configure Ad-hoc conferencing on the Avaya Communication Manager system:

1. Perform the following steps to administer Ad-hoc video ports on the Avaya Communication Manager system:
 - a. Use the **display system-parameters customer-options** command to access the Optional Features form.
 - b. On page 2 of the form, verify **Maximum Administered Ad-hoc Video Conferencing Ports**. The maximum number of Ad-hoc video conferencing ports allowed is the number of video ports available for Ad-hoc use on the MCU(s). For example, if you have three MCUs, and each MCU has 16 ports available for Ad-hoc use, the maximum number of Ad-hoc video conferencing ports allowed is 48.

Figure 38: Example of Page 2 of the Optional Features Form

```

135.64.26.170 - PuTTY
change system-parameters customer-options Page 2 of 2
OPTIONAL FEATURES

IP PORT CAPACITIES
Maximum Administered H.323 Trunks: 8000 62
Maximum Concurrently Registered IP Stations: 1221 7
Maximum Administered Remote Office Trunks: 8000 0
Maximum Concurrently Registered Remote Office Stations: 12000 0
Maximum Concurrently Registered IP eCons: 0 0
Max Concur Registered Unauthenticated H.323 Stations: 1000 0
Maximum Video Capable H.323 Stations: 1000 32
Maximum Video Capable IP Softphones: 1000 12
Maximum Administered SIP Trunks: 2000 865
Maximum Administered Ad-hoc Video Conferencing Ports: 16 16
Maximum Number of DS1 Boards with Echo Cancellation: 0 0
Maximum TN2501 VAL Boards: 10 0
Maximum Media Gateway VAL Sources: 250 0
Maximum TN2602 Boards with 80 VoIP Channels: 128 0
Maximum TN2602 Boards with 320 VoIP Channels: 128 3
Maximum Number of Expanded Meet-me Conference Ports: 0 0

(NOTE: You must logoff & login to effect the permission changes.)

```

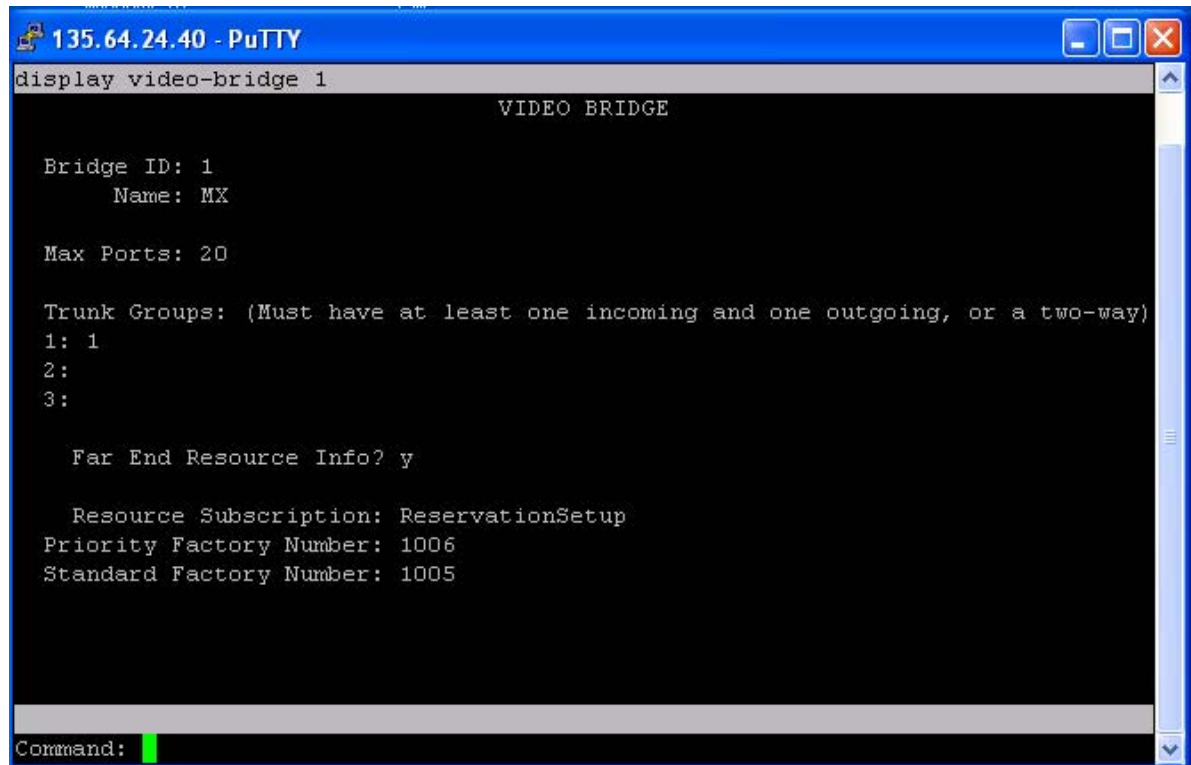
2. Perform the following steps to configure COS for the video ad-hoc-enabled users:
 - a. Use the **change cos** command to access the Class of Service form.
 - b. Go to page 2 of the form.
 - c. Set **Ad-hoc Video Conferencing** for the appropriate COS levels.
3. Perform the following steps to configure a video bridge on the Avaya Communication Manager system:
 - a. Use the **add video-bridge xx** command (where **xx** is the bridge number between 1 to 40) to access the Video Bridge form.
 - b. In **Name**, enter the name for this video bridge (for example, *Ad Hoc Video Bridge - Meeting Exchange*).
 - c. Set **Max Ports** to the maximum number of Ad-hoc conferencing ports you want to assign to this bridge. (The minimum you can enter is 3.) This is equivalent to the number of ports that are available for Ad-hoc use on the associated RMX based on a needed bit rate for video.

Setting Up Video Endpoints

- d. In **Trunk Groups**, enter the administered SIP trunk groups you added in [Procedure 5: Add a SIP Trunk Group for the Meeting Exchange System](#) on page 106.

The Far End Resource Info, Resource Subscription, Priority Factory Number, and Standard Factory Number fields appear.

Figure 39: Example of the Video Bridge Form



- e. Make sure **Far End Resource Info?** is set to **y**.
- f. Set **Priority Factory Number** to the number you specified in the file `conferenceProfile.cfg`.
- g. Set **Standard Factory Number**. to the number you specified in the file `conferenceProfile.cfg`.

Procedure 9: Configure Avaya SES for Meeting Exchange 5.0.1 S6800

To configure Avaya SES for Meeting Exchange:

1. Log into the Avaya SES Administration interface (<http://<ses-ipaddress>/admin>) and verify that the SES is set up as a Home/Edge proxy. Other configurations are possible with multiple SES proxies. Select **Server Configuration>System Properties**, and verify that SIP Domain is set to the domain name administered on the Avaya Communication Manager signaling group.
2. For each SIP station, add a user on SES. (Select **Users>Add.**)
3. Add a media server interface. (Select **Media Server>Add.**) Be sure to set the following parameters:
 - **Media Server Interface Name** to the Avaya Communication Manager node name for its CLAN.
 - **SIP Trunk Line Type** to TLS.
 - **SIP Trunk IP Address** to the IP address of the CLAN interface.
 - **Media Server Admin Address** to the IP address to access SAT.
 - **Media Server Admin Login** to init.
 - **Media Server Admin Password** to the init password.
 - **Media Server Admin Password Confirm** to the init password.

The following figures shows an example of the media server interface settings.

Figure 40: Example of the SES Media Server Interface Settings

The screenshot shows a web browser window titled "Edit Media Server Interface - Microsoft Internet Explorer". The address bar displays "https://135.64.24.47/admin/do/listacp/edit_acp_id=1". The page header includes the Avaya logo and "Integrated Management SIP Server Management" with the server address "135.64.24.47". A left sidebar contains a navigation menu with options like Top, Setup, Users, Conferences, Media Server Extensions, Emergency Contacts, Hosts, Media Servers, Address Map Priorities, Adjunct Systems, Trusted Hosts, Services, Server Configuration, Certificate Management, IM logs, Trace Logger, and Export/Import to ProVision. The main content area is titled "Edit Media Server Interface" and contains the following configuration fields:

- Media Server Interface Name***: CANAL
- Host**: 135.64.24.47
- SIP Trunk**
 - SIP Trunk Link Type**: ☐ TCP ☒ TLS
 - SIP Trunk IP Address***: 135.64.24.40
- Media Server**
 - Media Server Admin Address (see Help)**: [Empty field]
 - Media Server Admin Login**: [Empty field]
 - Media Server Admin Password**: [Empty field]
 - Media Server Admin Password Confirm**: [Empty field]
- SMS Connection Type**: ☒ SSH ☐ Telnet

Below the fields, it states "Fields marked * are required." and there is an "Update" button.

4. Create a media server extension for each SIP user you added that will be configured as OPTIM. This informs SES to route all signaling calls from that user to the media server (Avaya Communication Manager). Select **Media Server Extensions>Add**. Be sure to set the following parameters:

- **Extension** to the Avaya Communication Manager station to be associated with the user.
- **Media Server** to the media server that you created.

After creating the media server extension, map the media server extension to the user. (Select **Media Server Extensions>List Select <Assign> user ID** [the SIP user to map with this extension]).

SES must understand where to route each number originating from a SIP endpoint and destined to a non-SIP endpoint or trunk.

5. Configure Avaya Meeting Exchange as a trusted host in SES. (Select **Trusted Hosts>Add.**) Set **IP Address** to the IP address of the Avaya Meeting Exchange system.

Useful commands:

trustedhost usage:

trustedhost -L # list all third party trusted hosts currently configured

trustedhost -a trusted-host-IP-address -n trusting-SES-IP-address [-c 'comment text'] # add new trusted host

trustedhost -d trusted-host-IP-address -n trusting-SES-IP-address # delete a trusted host

trustedhost -N # List all SES host IP addresses

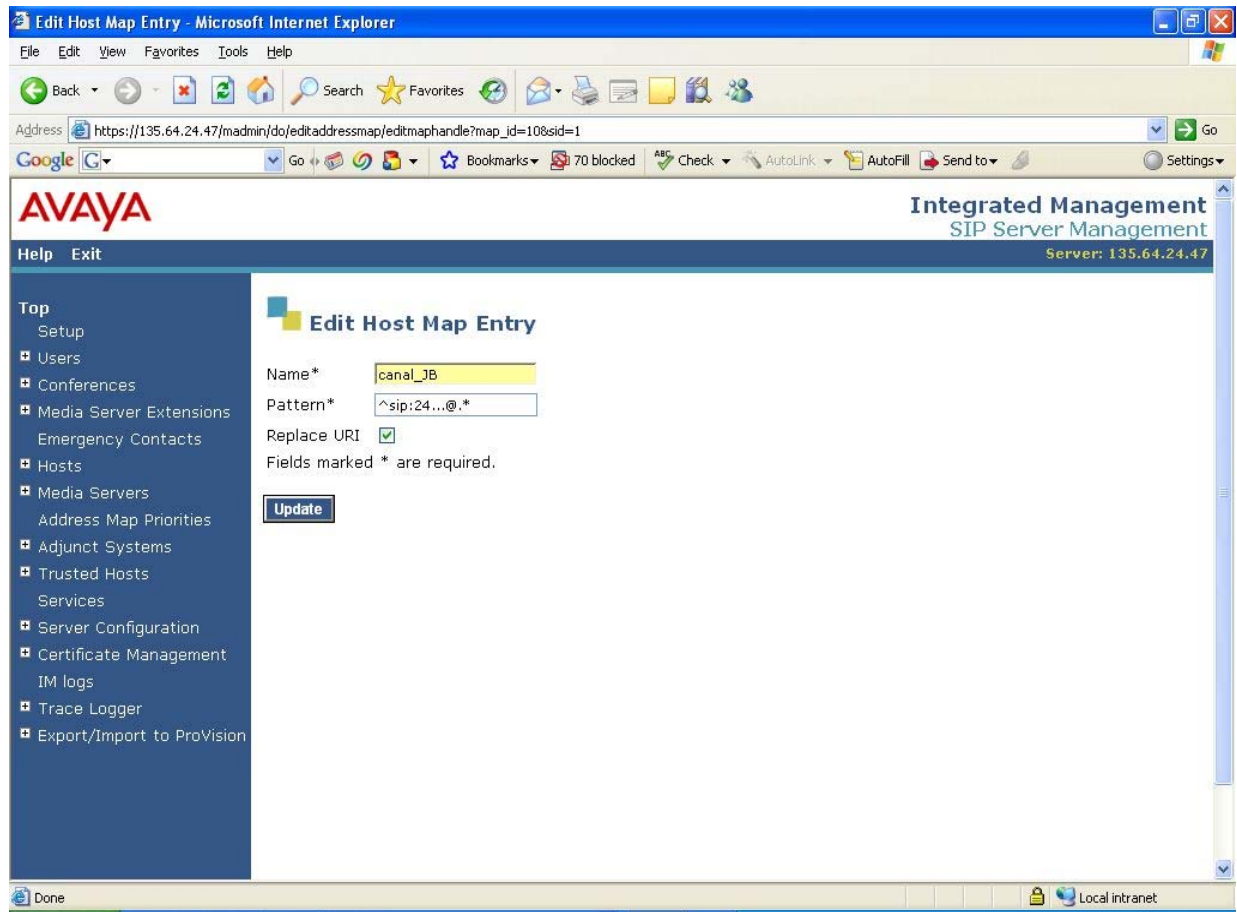
trustedhost -V # -v can be used with any option

6. Configure SES to redirect calls to Avaya Meeting Exchange. (Select **Hosts>List Add Map in New Group.**) Set the following parameters:

- Name to text that identifies the group.
- Pattern to a regular expression to match SIP extensions.

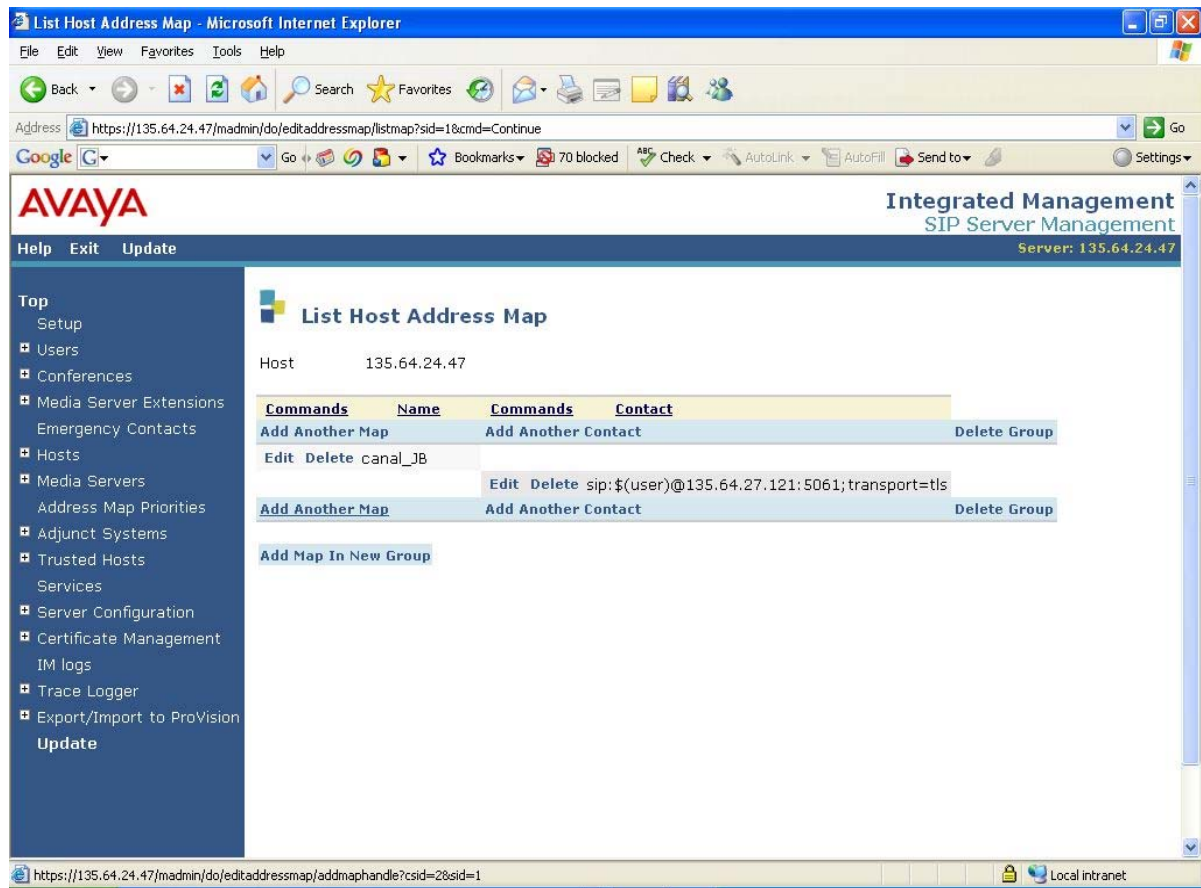
The following figures shows an example of the Edit Host Map Entry page.

Figure 41: Example of the SES Edit Host Map Entry Page



After completing the Edit Host Map Entry page, click **Add another Contact** and set **Contact** to the SIP address for the Avaya Meeting Exchange system (for example, sip:\$(user)@xxx.xxx.xxx.xxx:5060;transport=tls).

Figure 42: Example of the SES List Host Address Map Page



Configure a Polycom MGC Video Conferencing Bridge Platform as an H.320 Gateway

This section describes how to configure a Polycom MGC video conferencing bridge platform as an H.320 gateway.

Before performing the procedures in this section, make sure the MGC is already administered and registered to an Avaya Communication Manager system with inbound and outbound trunks correctly configured per the instructions in [Configure Polycom MGC Video Conferencing Bridge Platforms with Avaya S8500 and S87xx Server](#) on page 82.

Trunk Groups

If the MGC is set up with outgoing and incoming trunk groups, you must create one incoming trunk group that may map to many signaling groups with one signaling group per IP board. This trunk group is the “incoming and gateway” trunk group.

Set the following parameters for the incoming and gateway trunk group:

- **Direction** to **two-way**.
- **Service Type** to **tie**.
- **Disconnect Supervision - In?** to **y**.
- **Outgoing Display** to **y**.
- **Send Calling Number** to **y**.
- **Format** to **private**.

This incoming and gateway trunk group may consist of trunk members associated to many incoming and gateway ARQ+RRQ signaling groups. As result, the outgoing call traffic will spread across all signaling groups and IP boards.

Route Pattern

Use **add route-pattern xx** to create a new route pattern (a “Gateway Pattern”) per MGC Session Profile for H.323 to H.320 calls. The user will dial the dial plan prefix and the H.320/H.323 number. The route pattern will omit the dial plan prefix and add the string **XXYY*** before the H.323/H.320 number, where **XXYY** is the IP service prefix and the Session Profile prefix, and ***** is the delimiter required by the gateway function.

Using AAR tables, enable the user to access the AAR table via a facility code and then an Avaya Communication Manager gateway prefix is created per MGC Session Profile. Use **change aar analysis** to add a dial string and map to the route pattern you created.

The Avaya Communication Manager system does not support dial strings that contain the ***** character or the **#** character as required by the MGC to support H.320 gateway functionality.

AAR Tables

Using AAR tables, the user accesses the AAR table via a facility code, and then an Avaya Communication Manager gateway prefix is created per MGC Session Profile. Use **change aar analysis** to add a dial string and map to the route pattern you created.

MGC Administration

On the MGC, perform the following steps:

1. Under **Network Services>ISDN**, create the required ISDN service.
2. Under **Gateway Configuration>Session Profiles>To H.320 Session Profile**, create a profile with the matching E.164 as per the AAR table and route pattern, and assign an ISDN service. Ensure Transcoding is set to always.
3. Under **Gateway Configuration>Session Profiles>To H.323 Session Profile**, create a profile and assign the IP service that corresponds to an IP board/CLAN. Ensure Transcoding is set to always.
4. Change the delimiter to ***** instead of **#** or vice versa (that is, consistent administration between the route pattern and the MGC expected delimiter).

Configure a Polycom PathNavigator/SE200 Gatekeeper

This section describes how to configure a Polycom PathNavigator/SE200 Gatekeeper.

Checklist

When setting up these systems, you will need to know the following information:

- the IP codec sets you want to use
- the IP network regions you want use
- the IP address of the IP board for the gatekeeper

Configuration Procedures

To configure a Polycom PathNavigator gatekeeper, you must perform the following steps:

1. Add an entry in the IP Node Names for the PathNavigator/SE200.
2. Add a signaling group for the PathNavigator.
3. Add a trunk group for the PathNavigator.
4. Modify the signaling group for the PathNavigator.
5. Create a route pattern to the PathNavigator.
6. Configure the PathNavigator.

Procedure 1: Add an Entry in the IP Node Names for the PathNavigator/SE200

To add an entry in the IP Node Names form for the PathNavigator/SE200 system:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the PathNavigator/SE200 system.
3. In the corresponding IP Address field, enter the IP address of the IP board for the PathNavigator/SE200 system.

Procedure 2: Add a Signaling Group for the PathNavigator/SE200

To add a signaling group for the PathNavigator/SE200 system:

1. Use the **add signaling-group xx** command (where **xx** is the chosen signaling group) to access the Signaling Group form.
The Signaling Group form appears.
2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Priority Video**. If you want all incoming calls to receive priority video transmissions, select **y**.
5. Set **Near-end Listen Port** to **1719**.
6. Set **LRQ Required** to **y**.
7. Set **Far-end Node Name** to the name you entered for the PathNavigator/SE200 system.
8. Set **Far-end Listen Port** to **1719**.
9. Set the **Far-end Network Region** to the appropriate IP network region.
10. Set **Direct IP-IP Audio Connections** to **y**.
11. Set **IP Audio Hairpinning** to **y**.

Procedure 3: Add a Trunk Group for the PathNavigator/SE200

To add a trunk group for the PathNavigator/SE200 system:

1. Use the **add trunk-group xx** command (where **xx** is the chosen trunk group) to access the Trunk Group form.
The Trunk Group form appears.
2. Set **Group Type** to **isdn**.
3. Set **Carrier Medium** to **IP**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 4: Modify the Signaling Group

To modify the signaling group for the PathNavigator system:

1. Use the **change signaling-group xx** command (where **xx** is the signaling group you added) to access the Signaling Group form.
The Signaling Group form appears.
2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 5: Create a Route Pattern for the PathNavigator/SE200

To create a route pattern that points to the trunk group:

1. Use the **change route-pattern *xx*** command (where ***xx*** is the route pattern you want to use) to access the Route Pattern form.

The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the trunk group you created for the PathNavigator/SE200.

Procedure 6: Configure the PathNavigator/SE200

Follow the instructions provided with the system to install and configure the Polycom PathNavigator/SE200.

Configure Video Trunks between Two Avaya Communication Manager Systems

This section describes how to configure video trunks between two Avaya Communication Manager systems.

Checklist

When setting up these video trunks, you will need to know the following information:

- the IP address of the CLAN or PCLAN of the other Avaya Communication Manager system
- the IP network regions you want use

Configuration Procedures

To configure a video trunk between two Avaya Communication Manager systems, you must perform the following steps:

1. Add an entry in the IP Node Names for the video trunk.
2. Add a signaling group for the trunk.
3. Add the trunk.
4. Modify the signaling group.
5. Create a route pattern for the trunk.

Procedure 1: Add an Entry in the IP Node Names for the Video Trunk

To add an entry in the IP Node Names form for the video trunk:

1. Use the **change node-names ip** command to access the IP Node Names form.
2. In the Name field, enter a name for the video trunk.
3. In the corresponding IP Address field, enter the IP address of the CLAN or PCLAN of the other Avaya Communication Manager system.

Procedure 2: Add a Signaling Group for the Video Trunk

To add a signaling group for the video trunk:

1. Use the **add signaling-group xx** command (where **xx** is the chosen signaling group) to access the Signaling Group form.

The Signaling Group form appears.

2. Set **Group Type** to **h.323**.
3. Set **IP Video** to **y**.
4. Set **Near-end Listen Port**.
5. Set **LRQ Required** to **n**.
6. Set **Far-end Node Name**.
7. Set **Far-end Listen Port**.
8. Set the **Far-end Network Region**. If you set the maximum bandwidth for video calls in Procedure 3, assign that IP network region.
9. Set **Calls Share IP Signaling Connection** to **y**.

Note:

You must set this parameter to **y**.

10. Set **Direct IP-IP Audio Connections** to **y**.
11. Set **IP Audio Hairpinning** to **y**.

Procedure 3: Add a Trunk Group

To add a trunk group:

1. Use the **add trunk-group xx** command (where **xx** is the chosen trunk group) to access the Trunk Group form.

The Trunk Group form appears.

2. Set **Group Type** to **isdn**.
3. Perform one of the following steps:
 - For Avaya Communication Manager Release 3.01, set **Carrier Medium** to **IP**.
 - For Avaya Communication Manager Release 3.1 or later, set **Carrier Medium** to **H.323**.
4. Go to page 5 of the Trunk Group form.
5. Add members to the trunk group.

Procedure 4: Modify the Signaling Group

To modify the signaling group video trunk:

1. Use the **change signaling-group xx** command (where **xx** is the signaling group you added) to access the Signaling Group form.

The Signaling Group form appears.

2. Set **Trunk Group for Channel Selection** to the trunk group you just added.

Procedure 5: Create a Route Pattern for the Video Trunk

To create a route pattern that points to the trunk group:

1. Use the **change route-pattern xx** command (where **xx** is the route pattern you want to use) to access the Route Pattern form.

The Route Pattern form appears.

2. In the **Grp No** field, enter the number of the trunk group you created.

Monitor the Status of Video Bandwidth Usage

This procedure describes how to monitor the status of video bandwidth usage for inter-network regions.

Use the **status ip-network-region *x*** command (where ***x*** is the chosen IP network region) to view the video bandwidth usage. The current video bandwidth usage to each network region is displayed.

Use the **change ip-network-region *x*** command (where ***x*** is the chosen IP network region) to specify the maximum amount of bandwidth that can be used for video to each IP network region.

Index

A

Ad-hoc conferencing	
MGC systems	89
MGC-25 systems	89
RMX systems	71
Avaya Communication Manager	
configure video trunks.	131
Avaya Meeting Exchange	
configure	96
Avaya S8300 servers	78, 89
Avaya S8500 servers	82
Avaya S87xx servers.	82

H

H.320 gateway	
configure	126
HDX systems	
configure	57

I

IP Softphone	
configure	53

M

Meeting Exchange	
configure	96
MGC systems	
configure	82
configure Ad-hoc conferencing	89
MGC-25 systems	
configure	78, 89
configure Ad-hoc conferencing	89

P

PathNavigator gatekeeper	
configure	128
Polycom	
HDX systems	57
MGC systems	82, 89
MGC-25 systems	78, 89
PathNavigator gatekeeper	128
RMX systems	65, 71
SE200	128
V500 systems.	57
VSX systems	57
VSX700 systems	57
Polycom MGC	
configure as H.320 gateway	126

R

RMX systems	
configure	65
configure Ad-hoc conferencing	71

S

SE200	
configure	128

V

V500 systems	
configure	57
video conferencing systems	
configure	57, 65
configure Ad-hoc	71, 89
video trunks	
between Avaya Communication Manager systems	131
VSX systems	
configure	57
VSX700 systems	
configure	57

